Savoir où sont placées les caméras,
comment elles fonctionnent,
comment leurs images sont transmises et consultées
et comment les technologies évoluent,
c'est se donner des moyens concrets
de pouvoir, avec plus de confiance,
s'en prendre à la vidéosurveillance
et aux intérêts qu'elle protège.

PAS VUE PAS PRISE

CONTRE LA VIDEOSURVEILLANCE

Une carte collaborative pour repérer les caméras :
https://sunders.uber.space/



version 1

mai 2023

pasvuepasprise@riseup.net

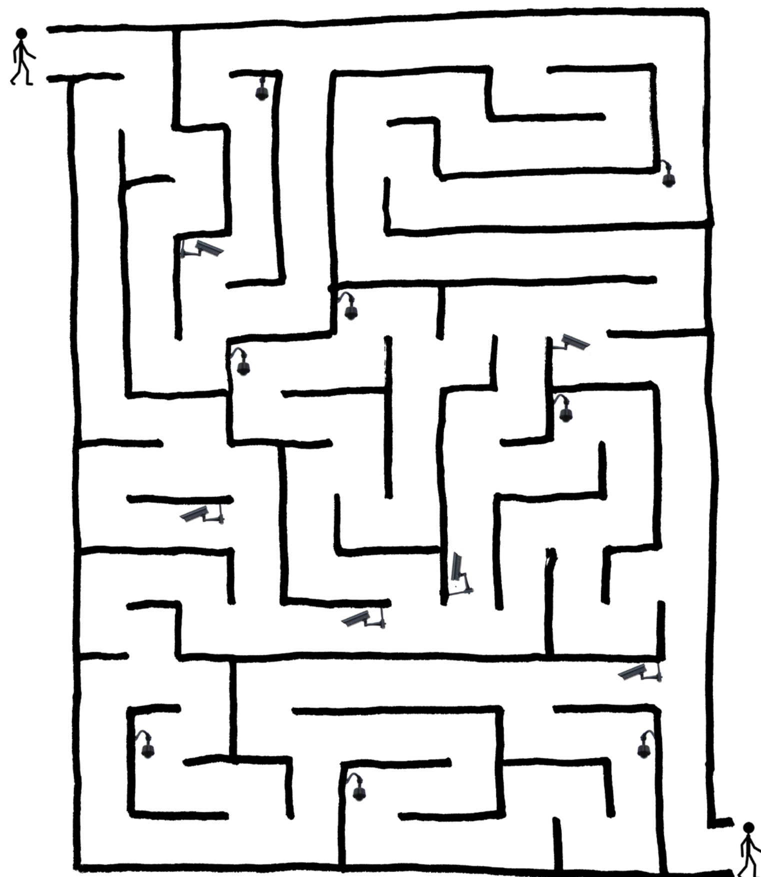


TABLE DES MATIÈRES

1. Introduction 4
2. Des rues de Levallois-Perret aux JO 2024 7
   2.1 Bref historique de la vidéosurveillance 7
   2.2 Les JO de la vidéosurveillance 14
3. Les différentes caméras 17
4. La qualité des images 23
   4.1 Quelle est la précision des caméras de vidéosurveillance ? 24
   4.2 Les caméras voient-elles vraiment la nuit ? 32
   4.3 Difficultés de maintenance et aléas techniques 35
5. Le centre de supervision urbain (CSU) 37
   5.1 Les opérateur-rice-s du CSU 39
   5.2 Les locaux de supervision 42
   5.3 Que font les opérateur-rice-s ? 43
   5.4 La mutualisation des systèmes de vidéosurveillance 46
6. Exploitation judiciaire des images 49
7. La vidéosurveillance automatisée (VSA) 51
   7.1 Les différents logiciels de vidéosurveillance automatisée 51
   7.2 La reconnaissance faciale 65
8. La vidéosurveillance en région parisienne 69
9. Esquiver et saboter les caméras 73
   9.1 S'attaquer à la caméra 74
   9.2 S'en prendre au support 76
   9.3 Saboter l'alimentation et les câbles de données 77
10. Liste d'entreprises 84
11. Ressources 88

1. INTRODUCTION



En quelques années la vidéosurveillance s'est imposée de manière incontournable dans notre quotidien. Les caméras ne sont plus réservées aux boulevards des villes ou aux allées des grands magasins, aujourd'hui on peut les croiser partout. Elles sont devenues banales au point qu'on ne les remarque presque plus. Pourtant, pour certain-e-s, difficile d'oublier le poids de ces petits appareils voyeurs sur nos vies et nos modes de fonctionnement. Elles rendent les endroits pris dans leur champ de vision plus hostiles, parce que, forcément, avoir l'impression d'être épié-e en permanence rend méfiant-e. On se demande si n'on a pas l'air louche, on s'auto-censure. C'est le propre de la surveillance que de pousser à la normalisation, de faire qu'on s'assagisse de soi-même par crainte d'une répression potentielle.

La « sécurité » par la répression et le contrôle c'est une des bases de l'État, qui reste toujours à la recherche de nouveaux moyens d'asseoir et de consolider sa domination. La vidéosurveillance, même si elle n'est qu'un outil parmi d'autres, prend une place de plus en plus importante dans la panoplie sécuritaire actuelle. Notamment parce que les caméras sont un soutien d'autres dispositifs pour un État qui ne peut pas multiplier les flics à l'infini. En augmentant constamment leur champ de vision et leur efficacité par des nouvelles installations et des logiciels de surveillance automatisée toujours plus performants, les condés peuvent accroître leurs capacités sans avoir à augmenter leurs effectifs. Qu'on ne se fasse pas d'idées pour autant, le déploiement croissant de vidéosurveillance dans l'espace public

AUTOUR DE LA SURVEILLANCE

- Technopolice : *https://technopolice.fr*
- Ears and eyes (en anglais) : *https://earsandeyes.noblogs.org/fr/*
- Centre de documentation sur la contre-surveillance : *https://www.csrc.link/fr/*

ATTAQUES, RÉFLEXIONS ET INFORMATIONS PLUS LARGES

- Les sites des réseaux Mutu et Indymedia
- Sans nom : https://sansnom.noblogs.org/archives/category/videosurveillance
- Attaque : https://attaque.noblogs.org/post/category/anti-cameras/

RESSOURCES TECHNIQUES

- Guides Pixels édités par AN2V (association défendant la vidéosurveillance)





Voici différentes ressources qui ont servi pendant l'écriture de cette brochure ou qui peuvent servir pour continuer à lutter contre la vidéosurveillance.

CARTOGRAPHIE DES CAMÉRAS

- Surveillance under surveillance : *https://sunders.uber.space/*
- MyOsMatic - pour imprimer ses propres cartes :
- En ligne : *https://print.get-map.org*
- Code source : *https://github.com/hholzgra/maposmatic/*
- Il existe aussi un site de cartographie français qui utilise sa propre base de données (qui n'est plus actualisée), avec des ressources : *https://www.sous-surveillance.net/*

BROCHURES, AFFICHES, TEXTES

- La rage contre la vidéosurveillance 2020-2021 : *https://infokiosques.net/spip.php?article1833*
- Affiches & visuels : *https://affiches.blackblogs.org/tag/videosurveillance/*

n'est pas synonyme d'une diminution du nombre de patrouilles de keufs dans la rue.

En plus d'être un pilier de la répression, la vidéosurveillance est aussi par essence un formidable outil de discipline. Son panoptisme, l'impression pour nous d'être possiblement observé-e-s partout et tout le temps, pousse à la normalisation. D'autant plus quand on sait que les logiciels de vidéosurveillance visent de plus en plus à détecter les comportements « anormaux »: s'arrêter dans un espace où il faut marcher, flâner alors que l'on devrait savoir où on va, s'asseoir là où il faut se tenir debout, se rassembler alors qu'il faudrait rester seul-e. Combattre la vidéosurveillance c'est aussi revendiquer de pouvoir vivre sans se demander encore plus à quelles normes il faut se soumettre alors qu'on voudrait les abolir toutes. On aurait tort de ne voir que les caméras de rue. Le regard du pouvoir vient s'immiscer dans tous les endroits où les forces de contrôle cherchent à se déployer : lieux de travail, écoles, prisons, halls d'immeuble, transports, etc. Partout l'État et ses auxiliaires cherchent à rappeler et à renforcer leur présence. Et comment ne pas voir toutes celleux qui installent des caméras chez elleux et dégaînent leur téléphone à la moindre anomalie ? De la manif à la rando, rares sont les endroits et les moments où l'on n'a pas à se méfier d'être épié-e-s par un petit mouchard.

Et comme on en a fait l'expérience pendant le confinement avec les drones, même la tranquillité de plages, de forêts et de montagnes se voit dérangée par leur bourdonnement arrogant.

Du coup le déploiement massif de caméras, leur perfectionnement et les promesses d'extension de leurs usages foutent la trouille. Ça paraît vertigineux. Mais on n'a pas envie de se résigner, ce n'est pas parce que la vidéosurveillance est devenue omniprésente qu'elle ne peut plus être remise en question et attaquée. En clair, on refuse de s'y habituer.

Malgré l'impression qu'on peut en avoir, ces systèmes sont loin d'être infaillibles, ils ont des points faibles, des brèches, et il existe plein de façons de les contourner. Alors l'idée de ce projet c'est de mutualiser nos connaissances, nos astuces et nos pratiques pour se

sentir plus fort-e-s, en se donnant des billes pour se débrouiller face à la vidéosurveillance. Pour qu'elle ne nous assomme pas au quotidien ni ne nous empêche d'agir.

Savoir où sont placées les caméras, comment elles fonctionnent, comment leurs images sont transmises et consultées et comment les technologies évoluent, c'est aussi se donner des moyens concrets de pouvoir, avec plus de confiance, s'en prendre à la vidéosurveillance et aux intérêts qu'elle protège.

Ce projet repose sur des connaissances acquises un peu partout par différentes personnes, il n'est donc pas l'oeuvre de technicien-ne-s ou d'expert-e-s. Ça veut dire qu'on ne prétend ni être complètement exhaustif-ve-s, ni qu'on n'a pas pu faire d'erreur dans ce que l'on partage et que, la situation évoluant continuellement, il y aurait sans cesse des ajouts et modifications à apporter. Mais ça veut aussi dire qu'il y a pas mal d'informations accessibles à celles et ceux qui veulent apporter de l'eau au moulin de la lutte contre la surveillance.

L'ETAT NOUS OBSERVE CREVONS LUI LES YEUX !





SECURITAS
124 Boulevard de Verdun
92411 Courbevoie

SENSIVIC
Le Lab'O, 1 avenue du Champ de Mars
45100 Orléans

SLAT
11 rue Jean Elysée Dupuy
69410 Champagne-ai-Mont-d'Or

SPIE CITYNETWORKS
1-3 place de la Berline
93287 Saint-Denis

STANLEY SECURITY FRANCE
2 Allée de l'Expansion,
69340 Francheville

SURVISION
22 rue d'Arras
92000 Nanterre

TECHNILUM
112 route de Maureilhan
34500 Béziers

TECHNIMAST
79 route de Caumont
84470 Châteauneuf de Dardagne

THALES
20-22 rue Grange Dame Rose
78141 Vélizy-Villacoublay

TIL TECHNOLOGIES
Parc du Golf - 350 rue de la Lauzière
13592 Aix-En-Provence

TRACOR EUROPE
13 rue des Pyrénées
91090 Lisses

VDSYS
799 rue du Docteur Calmette
(ZI TOULON EST)
83210 La Farlède

VIDETICS SAS
535 route des Lucioles Les Aqueducs B3
06560 Sophia Antipolis



GROUPE SCOPELEC
Rue Gay Lussac - ZI de La Pomme
31250 Revel

GROUPE SNEF
87 avenue des Aygalades
13015 Marseille

GTD INTERNATIONAL
1 chemin de la Coume
09300 Lavelanet

HCD
5 rue du Château
60440 Versigny

HIKVISION FRANCE
6 rue Paul Cézanne
93360 Neuilly Plaisance

HOLISEUM
5 place de la Pyramide
92088 Paris La Défense

INDEO
11 route du Sud- BP 27843
98863 Noumea - Nouvelle Caledonie

JUST DO IP
18 rue du Fort
92320 Châtillon

KONICA MINOLTA VIDEO-SOLUTIONS-SERVICES
365-367 route de Saint-Germain
78420 Carrière-sur-Seine

LOOPGRADE
4 avenue des 3 Peuples
78180 Montigny-le-Bretonneux

LUMATECH SOLUTIONS AND SERVICES
Avenue de l'Europe – Zone Eurolys
59280 Arementieres

MA2
2 rue de Rouen
95450 Vigny

MARCH NETWORKS
3-5 rue Saint Georges
75009 Paris

MOBOTIX AG
34 rue de la Croix de Fer
78100 Saint-Germain-en-Laye

NOMADYS
296 rue de la Béalière - Zone Actisud - Bât E
38113 Veurey-Voroize

ONET SECURITE TELEM
16 rue de l'étang - BP 01
38610 Gières

PANASONIC FRANCE
1-7 rue du 19 mars 1962
92230 Gennevilliers

PROMESSOR
100-101 quartier Boieldieu -Tour Franklin
92042 Paris La Défense

PRYNTEC - GROUPE TEB
RD974
21190 Corpeau

SECURE SYSTEMS
180 rue René Descartes
13100 Aix-en-Provence



2.1 BREF HISTORIQUE DE LA VIDÉOSURVEILLANCE

Le premier système de vidéosurveillance a vu le jour en 1942 pendant la Seconde Guerre Mondiale en Allemagne. Il fut installé pour surveiller le lancement de missiles balistiques tirés sur l'Angleterre. À partir de la fin des années 60 ce type de systèmes commence à être développé et commercialisé pour des usages civils et plus particulièrement pour surveiller l'espace public. En 1968, c'est dans la ville d'Olean aux Etats-Unis que des caméras sont installées pour la première fois afin de surveiller des rues. Puis, durant les années 80, le Royaume-Uni généralise des systèmes de vidéosurveillance urbains, à la suite d'attentats de l'IRA (groupe armé indépendantiste irlandais).

En France, les premières caméras de rues sont installées à Levallois-Perret (92) au début des années 90 par le maire Patrick Balkany, dans un cadre légal flou. L'initiative a fait l'objet de vives critiques, plusieurs plaintes ont été adressées à la commission nationale informatique et libertés (CNIL), même si les politiques sécuritaires avaient déjà le vent en poupe parmi les habitant-e-s de la commune. Par ailleurs le système, composé de 96 caméras, était cher et difficilement exploitable. Malgré tout, sans surprise, cette première expérience contribua à inscrire la vidéosurveillance dans le paysage politique français. Peu de temps après, en 1995, une loi fut promulguée pour fixer le cadre légal pour l'installation de caméras dans les lieux publics. Progressivement la vidéosurveillance s'est ensuite imposée comme un enjeu des politiques publiques. Lors des élections municipales de mars 2001 le thème de l'insécurité est très

présent et l'installation de caméras apparait comme une mesure phare de nombreux programmes électoraux. Par la suite cette dynamique ne cessera de s'accentuer, en particulier après les attentats du World Trade Center à New-York en septembre 2001.

Qu'est-ce que la CNIL ?

La commission nationale informatique et liberté est créée en 1978, en réponse au scandale médiatique suscité par le projet SAFARI (système automatisé pour les fichiers administratifs et répertoires des individus). Ce dernier, qui n'a finalement pas vu le jour, visait à centraliser des informations personnelles (Etat civil, santé, impôts, cadastre, etc) de l'ensemble de la population par le biais du numéro de sécurité sociale. Avec la CNIL, l'État a voulu rassurer en créant un garde-fou qui garantirait le « respect des libertés individuelles ». Cette commission peut notamment être saisie par toute personne souhaitant se plaindre d'un dispositif de vidéosurveillance. La CNIL peut aussi exercer un contrôle des installations a posteriori et demander à l'État leur suspension ou suppression si elles ne sont pas conformes à la loi. En réalité, en encadrant le contrôle, la CNIL n'est rien d'autre qu'un outil pour que chacun-e se fasse à l'idée d'être épié-e en permanence. En proposant régulièrement des adaptations du droit aux besoins de surveillance de l'État, cette institution a servi à légitimer des technologies de contrôle toujours plus intrusives et à participer à leur développement. Et à l'heure où la vidéosurveillance est présente partout, la loi JOP (jeux olympiques et paralympiques) d'avril 2023 remet en cause le peu de pouvoir de la CNIL. Cette dernière n'aura même plus le droit d'accéder aux systèmes de vidéosurveillance. Les recours pour la destruction d'images nous concernant ou contre un système de vidéosurveillance se feront par le biais de commissions départementales de vidéoprotection et non plus sous le regard de la CNIL.

CITEOS VINCI ENERGIES
23-27 rue Delarivière-Lefoullon
92800 Puteaux

CYCLOPE.AI
6 place du Colonel Bourgoin
75012 Paris

DERICHEBOURG – TECHNOLOGIES
22 rue Alexandre Parodi
75010 Paris

DAHUA TECHNOLOGY FRANCE
8 rue Eugène et Armand Peugeot
92500 Rueil-Malmaison

DEVERYWARE
43 rue Taitbout
75009 Paris

DIGITAL ÉQUIPEMENT
25 rue Raymond Aron
76130 Mont-Saint-Aignan

EBOO SOLUTIONS
Immeuble Le Périphérique
11 av. des vieux moulins
74000 Annecy

EDICIA
1 rue Célestin Freinet
44200 Nantes

EET FRANCE
38 rue Mozart - 2 e Étage
92110 Clichy

EIFFAGE ENERGIE SYSTEMES
3-7 place de l'Europe
78140 Veilizy-Villacoublay

ENGIE SOLUTIONS INEO INFRACOM
72 avenue Raymond Poincaré
21000 Dijon

ERYMA
143 avenue de Verdun
92130 Issy-les-Moulineaux

EVITECH
3 rue Buffon
91400 Orsay

EXAVISION
ZAC Trajectoire - 8, Avenue Ernest Boffa
30540 Milhaud

FAIVELEY TRANSPORT
Immeuble CLEVER, Hall Garden, Bât 6A 3
Rue du 19 mars 1962
92230 Gennevilliers

FOXSTREAM
6 rue du Dauphiné
69120 Vaulx-en-Velin

GENETEC EUROPE
6-8 rue Daru
75008 Paris

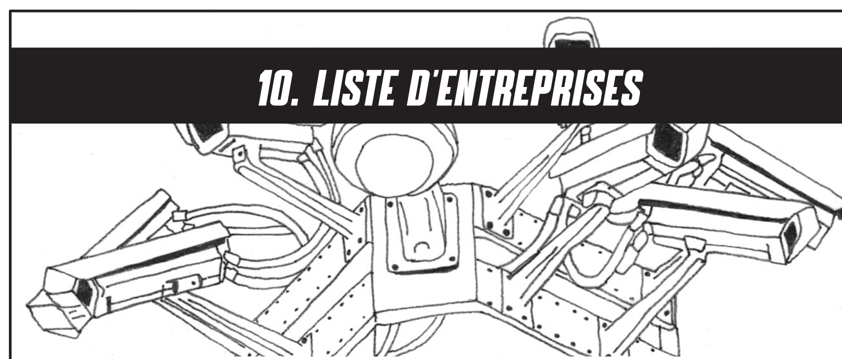
GIORDANA INGENIERIE
10 allée des Marronniers
69360 Ternay

GOSECURE
71 boulevard national
92250 La Garenne-Colombes

GROUPE PERIN SÉCURITÉ
73 rue des forges Saint Charles
08000 Charleville-Meziers







10. LISTE D'ENTREPRISES

Liste des entreprises (qui ont des adresses en France) :

4G TECHNOLOGY
460 avenue de la Quièra - ZA L'Argile Lot - 105 Voie C
06370 Moulans Sartoux

ADVANCED PROJECTS CONSULTING
2 rue Gustave Eiffel
10430 Rosières-près-Troyes

ASCALONE PROTEC INTELLIGENCE
12 rue du Prieuré
69130 Ecully

AXIS COMMUNICATIONS
42/46 avenue Aristide Briand
92220 Bagneux

AZUR SOFT
44 bvd Napoleon 3 - Bâtiment Le Tamango
06200 Nice

AZUR DRONES
2 rue Vert Castel
33700 Merignac

BOSCH SECURITY AND SAFETY SYSTEMS
126 rue de Stalingrad
93700 Drancy

BOUYGUES ENERGIES ET SERVICES
Immeuble atlantis
1 avenue Freyssinet
78280 Guyancourt

CABINET D'AVOCATS DU MANOIR DE JUAYEW
5/7 rue Georges Berger
75017 Paris

CAP SECURITÉ
27 rue Honoré Pététin
69700 Givors

CAMTRACE
1 allée de la Venelle
92150 Suresnes

CASD
ZA Actipole - 296 Rue de la Béalière
Bâtiment E - 38113 Veurey-Voroize

En 2006, Sarkozy, ministre de l'intérieur à l'époque, fait voter une loi relative à la lutte contre le terrorisme, qui assouplit les conditions d'utilisation de la vidéosurveillance dans l'espace public. C'est également l'actualité de la menace terroriste qui sera mise en avant pour justifier le lancement, en 2007, d'un plan national d'équipement de la « vidéoprotection ». On remarque au passage le changement sémantique qui, s'il n'a aucun effet sur la réalité de la surveillance, témoigne de la volonté de la rendre plus acceptable voire désirable. On préfère toujours être protégé-e que surveillé-e !

La même année est créé le fond interministériel de prévention de la délinquance (FIPD) pour inciter les collectivités locales à installer des caméras dans l'espace public. Avec cette caisse, dont l'argent est issu des amendes forfaitaires, l'État subventionne, entre autres, les projets d'installation de caméras et le raccordement des centres de supervision urbains (CSU) (cf. partie 5) aux services de police et de gendarmerie. En 2007, on comptait environ 20 000 caméras de surveillance des voies publiques. Selon les chiffres du ministère de l'Intérieur, entre 2007 et 2014, 2820 communes et 173 établissements publics de coopération intercommunale (EPCI) ont été subventionnés par le FIPD pour installer 26 614 caméras supplémentaires.

La multiplication des systèmes de vidéosurveillance va de pair avec leur banalisation. D'une part, le cadre légal s'affine comme dans la loi Loppsi 2 votée en 2011 (Loi d'orientation et de programmation pour la performance de la sécurité intérieure). Elle étend la liste des finalités justifiant la vidéoprotection des lieux publics et permet aux préfets d'installer temporairement des caméras lors de manifestations. D'autre part, les villes qui n'avaient jusque là pas de caméras subissent de plus en plus de pression pour en mettre. Par exemple, la commune de Villeurbanne (69), face au discours de Sarkozy la désignant comme « zone blanche » et à l'insistance des villes voisines, des gendarmes, des commerçant-e-s, et de citoyen-ne-s (sans doutes « vigilant-e-s »), finit par installer ses premières caméras en 2018 et en comptait 105 en 2021.

Après les attentats de Charlie Hebdo et du 13 novembre 2015, la menace terroriste sert à nouveau de prétexte pour justifier la mise en place de mesures de contrôle. Alors qu'est déclaré l'État d'urgence, le développement de la vidéosurveillance s'accélère. À Paris, entre 2015 et 2022, le nombre de caméras publiques dans les rues a quadruplé. Mais c'est aussi de plus en plus de petites communes qui deviennent vidéosurveillées.

Quelques exceptions

Il y a quelques rares contre-exemples de villes sans caméras publiques sur la rue : on peut citer, Ivry-sur-Seine, Vitry-sur-Seine, Fontenay-sous-Bois, Brest et Saint-Paul à la Réunion.

A contrario, si les villes les plus vidéosurveillées de France le sont par des mairies de droite, entre 2013 et 2020 les 13 nouvelles villes qui ont installé des caméras, le sont par des mairies de gauche.

À Nice, lorsque se produit l'attentat du 14 juillet 2016, la ville est déjà la plus vidéosurveillée de France. Selon les autorités locales, si les caméras n'ont pas empêché le massacre, c'est parce qu'il n'y en avait pas assez. La cadence d'installation prend donc un rythme plus soutenu, faisant augmenter leur nombre de 1300 en 2016 à 3300 en 2020. La ville déploie en parallèle le projet de « safe city », une ville connectée où vidéosurveillance et big data « veillent » sur la sécurité de tous-tes, à grand renfort de logiciels de surveillance automatisée en partenariat avec l'entreprise Thales. En 2019, Nice expérimente la reconnaissance faciale. Dans la foulée, la CNIL s'empresse d'exiger un encadrement juridique de cette technologie. On voit bien ici comment cette institution sert avant tout à démocratiser des moyens de contrôle toujours plus performants.

Les investissements publics attirent sans surprise une cohorte de boîtes privées pressées de se faire du fric sur ce marché en plein essor (cf. partie 10). Parmi les leaders du secteur on peut citer Axis ou Hikvision pour l'installation, Engie Ineo et Briefcam pour le traitement et l'analyse de données. Ces entreprises sont bien aidées par l'État qui accorde la loi avec leurs intérêts économiques et qui

Quelques tutoriels :

- Vidéo cartographie sur le terrain avec l'application StreetComplete : *https://video.antopie.org/w/e6f0b19f-c04f-4590-a40a-5f2d93a2a8c3*
- Vidéo cartographie sur ordinateur avec OSM et Sunders : *https://video.antopie.org/w/545dd83a-43a0-43d1-b38a-8a7b985dd89a*
- Tutoriel brochure Technopolice : *https://technopolice.be/wp-content/uploads/2021/07/guide_carto_technopolice_be-conv.pdf*





besoin. Il ne reste plus qu'a selectionner sa taille de papier et de soumettre. Attention, les cartes restent enregistrées...

Alors justement, comment contribuer soi-même à cette carte collaborative ? Il existe des applications pour smartphone comme Vespucci qui permettent de cartographier directement sur son téléphone, mais il est aussi très simple de relever des caméras en les notant précisément sur un plan avant de les enregistrer tranquillement depuis un ordinateur plus tard avec TOR et un compte OSM anonyme.

Pour cela, il faut donc se créer un compte dédié sur OSM (https://www.openstreetmap.org). Il existe quelques petits tutoriels pour se familiariser en général avec la cartographie, et en particulier avec l'ajout de caméras. Mais en gros on peut ajouter une caméra en zoomant précisément sur la zone concernée sur un fond de carte à choisir (image satellite ou plan). Il faut alors cliquer sur « Modifier » et choisir l'éditeur Id, pour pouvoir ajouter un point à l'endroit précis où se trouve la caméra. Il apparaît alors une fenêtre qui nous permet de renseigner l'attribut du point, en l'occurence il faut choisir « Caméra de surveillance » (désignée par le tag « man_made=surveillance »). Il est alors possible d'ajouter d'autres informations comme le type de caméra, l'orientation, ou s'il s'agit d'une caméra de ville ou privée. Mais même sans tous ces détails il est utile de signaler une caméra. Après avoir renseigné une ou plusieurs caméras, en faisant bien attention à ne pas modifier le reste de la carte, il faut sauvegarder ses modifications. Une nouvelle fenêtre s'ouvre, elle permet d'ajouter un éventuel commentaire et de vérifier dans le récapitulatif de nos modifications, si on n'a pas fait d'erreur. On confirme, et ça y est, la contribution est envoyée sur OSM. Elle apparaîtra très vite sur Surveillance under surveillance. Bravo !

promeut les partenariats public-privé. En 2020, les ventes cumulées des fabricants de dispositifs de vidéosurveillance (matériels et logiciels), distributeurs et installateurs, dans le cadre de marchés publics, atteignent près de 300 millions d'euros. Certaines entreprises font même des offres promotionnelles pour vendre leurs produits aux collectivités locales.

Promos sur les cams !

En 2017 Huawei offre 240 caméras « nouvelle génération » à la ville de Valenciennes (59). C'est le jackpot pour cette ville « pauvre » car le système de surveillance devient gratuit. Et ça l'est encore plus pour l'entreprise qui peut tester ses nouveaux modèles, expérimenter des logiciels de reconnaissance faciale pourtant interdite dans ce cadre, et se servir de la ville comme d'une vitrine pour ses nouveaux produits. De même, à Brienon-sur-Armançon, dans l'Yonne (3300 hab., 29 caméras), la municipalité a signé une convention de partenariat avec l'entreprise chinoise Dahua Technology en 2019. La facture pour la municipalité a été réduite en échange d'une promotion des produits de cette entreprise auprès des collectivités voisines.

Avec la crise sanitaire du covid-19 de nombreuses sociétés de sécurité ont saisi l'oppurtunité pour proposer des solutions de surveillance numérique. Par exemple, à Cannes et à Paris, pendant le confinement, l'entreprise Datakalab a experimenté un logiciel de détection du port du masque. La CNIL, une fois de plus, a poussé à une adaptation des réglementations en vigueur pour légaliser ce type d'outil, en pointant du doigt sa non-conformité avec la loi. Par ailleurs, avec la crise sanitaire on a vu se répandre les caméras thermiques pour contrôler la température des gens aux entrées des aéroports, des écoles, des entreprises ou des pôles administratifs. D'autres villes ont fait voler des drones pour diffuser des messages et appuyer les opérations de police en filmant depuis les airs (cf. partie 3).

La menace terroriste, la lutte contre la délinquance ou celle contre le covid, sont des épouvantails que les autorités agitent pour mieux faire accepter la vidéosurveillance et accélérer son déploiement. Qu'on se le dise, probablement que sans attentats ni crise sanitaire, la tendance aurait été sensiblement la même. Car, quoiqu'il arrive, la vidéosurveillance se présente pour l'État comme une formidable aubaine en vue de renforcer l'une de ses raisons d'être : contrôler les individus. Régulièrement il cherche à repousser les limites de l'acceptabilité de son contrôle sur nos vies, à l'aide de mécanismes désormais bien rôdés : des expérimentations pionnières suscitent un taulé, des critiques sont formulées avant d'être intégrées dans une loi qui légalise le nouveau dispositif, tout en laissant croire que rien n'a changé, qu'on serait toujours aussi libre qu'avant.

Les champions de la vidéosurveillance dans l'espace public

À titre de comparaison avec le reste du monde, la ville la plus vidéosurveillée d'Europe est Londres, où l'on trouve près de 7 000 caméras pour 100 000 habitant-e-s selon une étude de Comparitech publiée en 2019. Quant au titre mondial, il revient à la ville chinoise, Chongqing, qui compte 16 800 caméras pour 100 000 habitant-e-s, soit une pour 6 habitant-e-s en moyenne. Nice, la ville la plus vidéosurveillée de France, comprenait, en 2019, un total de 2666 caméras, soit 771 caméras pour 100 000 habitant-e-s.

Le développement de la vidéosurveillance ne s'est pas fait sans rencontrer de résistance. Et si on ne peut pas dire qu'il y a eu un large mouvement pour s'y opposer, on ne peut pas non plus ignorer les initiatives et les luttes contre les caméras. Beaucoup de ces résistances se sont exprimées et continuent de le faire sous un prisme légaliste : des associations de riverain-e-s ou de défense des droits de l'homme dénoncent l'installation ou la présence de dispositifs de vidéosurveillance par des campagnes publiques et/ou des recours juridiques.

Cartographie

Si le site de cartographie collaborative OpenStreetMap (OSM) permet aux utilisateur-ice-s de cartographier une multitude de choses, et notamment les caméras, elles ne sont pas toutes visibles sur la carte de base. C'est pourquoi il faut passer par des sites qui extraient ces données d'OSM pour les restituer toutes sur une nouvelle carte vierge.

Surveillance under surveillance (https://sunders.uber.space/fr/) en est un. Toutes les heures, il extrait automatiquement les données sur les caméras du monde entier documentées sur OSM. En zoomant sur une zone on peut donc voir l'emplacement précis des caméras signalées. Évidemment, les données sont issues de relevés sur le terrain, et certaines zones peuvent avoir été complètement ratissées alors que d'autres n'ont jamais été explorées. L'absence de caméras sur la carte n'indique donc pas forcément une absence dans la réalité. Ça donne quand même une idée, d'autant qu'à l'écriture de cette brochure en 2023, plusieurs milliers de caméras sont cartographiées en région parisienne par une multitude de contributeur-ice-s. Il est d'ailleurs possible d'imprimer des cartes avec les caméras grâce à MapOSMatic par exemple (https://print.get-map.org/).

Pour cela, plusieurs réglages sont possibles. Le premier réglage est la taille de la carte. Une carte de 4km sur 4km sera tout juste lisible sur un A3 (« full layout without index »), 8km sur 8km sera très lisible sur un atlas (« a multi-page layout »), et on peut pousser jusqu'a 16km sur 16km. Ensuite il faut selectionner le mode d'imposition, pour ne pas s'embêter avec les index, «health related facilities» n'en ajoute pas. Le reste parle plutot de lui même, comme fond de carte, «french OSM style» semble très lisible. L'onglet couche, ajouter «surveillance cameras» et «scale bar» pour avoir une echelle si



Chercher ailleurs

23 mai 2021, Saint-Denis (banlieue parisienne) Nathalie Voralek, adjointe à la ville de Saint-Denis en charge de la sécurité et de la tranquillité publique, retrouve sa voiture avec le pare-brise enfoncé. Un acte de vandalisme qui n'est pas le premier puisque l'élue a déjà retrouvé sa voiture avec les pneus crevés. Un entêtement qui ne doit rien au hasard selon elle. Cette nouvelle dégradation intervient deux jours à peine après l'inauguration du nouveau Centre de supervision urbaine (CSU) de la ville et ses 93 caméras.

Certain-e-s peuvent aussi aller plus loin en amont : saboter les chantiers d'installation avant que les caméras ne soient opérationnelles, chercher les entreprises qui les installent et s'y attaquer ou à leur stock, rendre visite aux élu-e-s qui financent la vidéosurveillance et décident de nous espionner, etc.



Avec la multiplication des caméras, d'autres formes de contestation ont vu le jour. Un outil contre la vidéosurveillance a souvent été de cartographier les caméras présentes dans l'espace public que ce soit pour les éviter, les saboter, ou juste montrer l'ampleur de leur présence. De manière parfois plus discrète, au cours de leur installation il y a eu des campagnes de sabotage, et régulièrement depuis leur mise en place, elles sont détruites ou dégradées, parfois de manière visible au cours de manifestations (cf. partie 9). Ces luttes se sont accompagnées de nombreuses campagnes d'affichage contre la vidéosurveillance (cf. à côté et p.6).

2.2 LES JO DE LA VIDÉOSURVEILLANCE

Aujourd'hui les industriels de la sécurité se frottent les mains en vue des JO 2024 de Paris, énième prétexte qu'utilisent l'État et les autorités locales pour renforcer le contrôle dans les rues et l'espace public. On a pu le voir dans d'autres pays, par exemple à Tokyo pendant les JO 2020, où la reconnaissance faciale a été autorisée dans certains espaces. En France, elle a aussi été autorisée à titre d'expérimentation en 2019 et testée à plusieurs reprises avec plus ou moins de réussite, notamment en 2020 à l'entrée du stade de Metz et lors du tournoi de Roland Garros. Son déploiement étant toujours interdit en France, les entreprises du secteur qui par ailleurs voient depuis quelques années leur chiffre d'affaire considérablement augmenter (Thales, Idemia, IBM, XXII, etc) mettent la pression en faveur d'un assouplissement de la loi. Au final, la reconnaissance faciale ne sera pas utilisée pendant ces JO, mais la deuxième loi JOP (jeux olympiques et paralympiques)[1] va rendre légal l'usage de la vidéosurveillance automatisée à titre expérimental - technologie qui, comme on le verra dans la partie 7, et contrairement à ce que pourrait laisser penser cette légifération, est déjà largement utilisée.

Cette loi ne concerne pas seulement le moment et les infrastructures des JO, par exemple en réduisant dès maintenant les prérogatives de la CNIL. Bien que certaines mesures soient censées ne concerner que la durée des JO, on peut s'attendre à ce qu'elles soient utilisées en amont ou perdurent par la suite. Ce sera peut-être le cas pour l'installation de scanners corporels à l'entrée des stades (malgré leurs coûts très élevés qui dissuadent même l'organisation des JO), la facilitation du travail le dimanche, l'assouplissement des règles sur la publicité, la nomination du préfet de paris comme seul responsable de la sécurité sur toute l'Ile-de-france, la multiplication des enquêtes sur les travailleur-euse-s ou les participant-e-s aux JO, mais aussi la vidéosurveillance automatisée (VSA).

1 La première loi JO de 2018 concernait essentiellement les aspects financiers et urbanistiques.

Sur la piste des cables

Limoges, dans la nuit du 9 au 10 septembre 2022. Vers 1 h 15, un ou plusieurs individus auraient mis le feu à des câbles souterrains, en soulevant des plaques situées sur les trottoirs, et à des boîtiers électriques d'immeubles, du côté de l'allée Manet. Ces incendies criminels ont eu pour conséquence de perturber le fonctionnement des feux de circulation et, surtout, de mettre hors d'état de fonctionner les caméras de vidéoprotection du secteur, ce qui était probablement le but de l'opération.

Il est possible de trouver les interrupteurs des lampadaires du quartier, qui sont souvent sur la même borne électrique. Ça a l'avantage de ne pas agir sous la caméra ciblée, et de plonger, en prime, le coin dans le noir. Si malheureusement le circuit électrique n'est pas le même, le manque de lumière complique tout de même l'action des caméras.

Suivant les villes, les images sont centralisées dans un CSU. Partir des câbles de données d'une caméra pour y remonter, ou partir du CSU pour trouver une trappe où toutes les données des caméras de la ville transitent est une piste. Souvent, un réseau dédié existe, et parfois c'est même écrit sur des badges enserrant les câbles, de manière pas forcément claire, mais par déduction... Au pire le coin est libéré de l'aliénation d'internet, donc du télétravail et du paiement dématérialisé en rab !



Incendier

Un communiqué sorti sur internet nous apprend que dans la nuit du 17 au 18 octobre 2022, 8 ***caméras ont été détruites par le feu*** *lors d'une action coordonnée dans le centre de Marseille.*

La nuit du 22 au 23 juillet 2022, à Chatellerault, deux caméras ont été endommagées par ***des feux de poubelles à la base du poteau*** *soutenant le dispositif.*

À Roubaix, le 23 avril 2022, vers 2 heures du matin, les policiers municipaux de garde ont assisté à une scène plutôt hallucinante. Sur leurs écrans, ils ont vu un drone auquel était attaché un « filin enflammé » évoluer près d'une caméra pour tenter de la détruire.

Ouvrir les trappes dans les mâts et déposer un objet inflammable est une technique assez efficace, le mât agissant comme une cheminée. Il faut laisser de l'air pour que le feu n'étouffe pas en laissant la plaque ouverte.

Des poubelles en feu sous une caméra peuvent aussi affaiblir suffisamment le mât et provoquer assez de fumée pour que la caméra ne voie plus.

Lorsque la trappe est au sol, vérifier qu'elle ne baigne pas dans l'eau et alors la même technique peut être réalisée, le but étant de faire prendre les gaines en caoutchouc, par exemple avec du tissu imbibé d'un carburant.





D'autres lois plus ou moins justifiées par l'approche des JO ont déjà permis des mesures sécuritaires, concernant aussi la vidéosurveillance, par exemple la loi drone 2 (cf partie 3). Mais cette dernière loi permet de nouvelles possibilités et expérimentations en terme de VSA[2]. Et ce grâce à des algorithmes d'intelligence artificielle qui permettront de détecter des « situations anormales, des départs de feux, des colis abandonnés, des goulots d'étranglement de population », « en ciblant des personnes répondant à certains signalements ou encore des catégories de gestes comme la dégradation des biens publics ». Les logiciels pourront signaler ces comportements et analyser les images. Les choix des comportements suspects et les zones concernées seront décidées par décrets. Ils se baseront certainement sur les mêmes critères que les contrôles de flics dans la rue, par exemple en repérant automatiquement des personnes qui zonent longtemps au même endroit ou des groupes[3]. Cela concernera les lieux qui accueilleront les compétitions des JO mais aussi la coupe du monde de rugby de 2023, considérée comme un test sécuritaire avant les JO. Le préfet pourra aussi autoriser l'utilisation de la VSA pour tout évènement sportif, cuturel ou festif qui en fera la demande, et qui devra ensuite être validé par décret. La durée de conservation des images utilisées pour l'expérimentation sera de un an.

---

2 Voir la brochure de Technopolis « Paris 2024 : Les olympiades sécuritaires des Jeux Olympiques ».

3 Comme lors d'éditions précédentes les personnes dans la rue ont été déplacées définitivement ou momentanément voire à certaines époques enfermées. Les logiciels vont donc sûrement être très utilisés en amont et pendant les JO, pour fliquer les personnes dans la rue et empêcher l'installation de campements.

Les images des drones pourront aussi être utilisées avec la VSA. Des entreprises de transports publiques pourront les mettre en oeuvre, comme la SNCF et la RATP sur leurs caméras. L'application de ces logiciels passera d'abord par une phase de test dans ces lieux et évènements en direct, ou à partir de n'importe quelles images de vidéosurveillance s'apparentant à ces évènements et pourra ensuite être experimentée et mise en place jusqu'à fin mars 2025, alors que la durée des JO est de deux mois. Mais comme de nombreuses mesures exceptionnelles ou expérimentales, elles seront ensuite amenées à perdurer et être légalisées.

Les JO et cette loi sont l'occasion de vendre ces logiciels et de faciliter leur financement et les intégrer au matériel de vidéosurveillance dans de nombreuses villes. On imagine bien qu'aucune collectivité n'aura intérêt à s'en séparer par la suite.

Par ailleurs, plusieurs des collectivités où se dérouleront les JO s'organisent pour renforcer leur arsenal sécuritaire avec l'aide de l'État, qui en général finance à hauteur de 50% les caméras dans les villes par le biais de fonds qui filent de la tune pour ça (SEPD : rural ; FIPD : ville), avec du matériel qui est souvent déjà livré avec la VSA. À Saint-Denis, un centre de supervision urbain flambant neuf a vu le jour en 2021. Le réseau, doté en 2022 de 93 caméras, va être élargi pour atteindre les 500 caméras d'ici 2024 et les élus locaux planifient de doter la vidéosurveillance d'intelligence artificielle pour automatiser la constatation des infractions. Le ministère de l'intérieur a annoncé vouloir ajouter 500 caméras à Paris, et 330 à Marseille (où se dérouleront les épreuves nautiques), en tout 44 millions d'euros dédiés au FIPD.

À BAS LES JO !

9.3 SABOTER L'ALIMENTATION ET LES CÂBLES DE DONNÉES



Une trappe est très souvent présente dans le mât à hauteur humaine. D'autres fois surelevée, il faut alors trouver une poubelle ou un semblant d'échelle pour s'y hisser. Les trappes sont d'environ 30 centimètres sur 10 et s'ouvrent avec, selon les modèles, une clef Allen de taille 5 ou 6 ou bien une clef triangle d'électricien (qui peut parfois se remplacer par une clef à pipe, généralement de 10). Si la serrure semble trop compliquée, le loquet est souvent peu résistant, et à l'aide d'un tournevis plat et d'un pied de biche il peut être facile de le tordre ou de le faire tourner. Il arrive régulièrement que cette trappe soit soudée, voire inexistante sur certains modèles. Il faudra alors trouver la trappe au sol la plus proche. Souvent, en ville, les tranchées de goudron qui ont acheminé les câbles sont visibles, il suffit de la remonter, et d'ouvrir la plaque au sol. Parfois, ils posent des plots en béton dessus pour empêcher de l'ouvrir.

Sectionner

Une pince coupante aiguisée suffira à couper les câbles. Une pince avec des poignées en plastique est nécessaire dans tous les cas, plus ses bras sont longs plus c'est sécurisant. Avec des gants isolants en plus, c'est mieux ! Pour réduire le risque d'arc électrique, l'alimentation peut parfois être coupée en éteignant un disjoncteur qui se situe dans la même trappe. Sectionner le câble où le courant passe fera un bruit sourd et un flash qui peut éblouir. C'est possible que la rue disjoncte. Couper au plus ras, en haut et en bas, rend plus difficile la reconnexion, notamment si l'on sectionne aussi la fibre optique, si c'est ce moyen de transmission qui est utilisé. C'est un câble plus fin et non rigide, qui est fait de dizaines de fils microscopiques, que les technicien-ne-s devront recoller un à un, ou en tirer un nouveau en entier. De plus, la coupure de la fibre ne produit pas d'arc électrique ni de bruit.



9.2 S'en prendre au support

Arracher

Certain-e-s passent un câble entre la caméra et son support, rassemblent potentiellement avec un noeud les deux extrémités du câble et tirent. Envisageable en manif' car il y a du monde, ou à moins en s'aidant de la force d'un véhicule pour tirer le câble. Souvent la jonction entre le mât et la caméra lâche, mais il arrive que des poteaux se couchent !



Scier

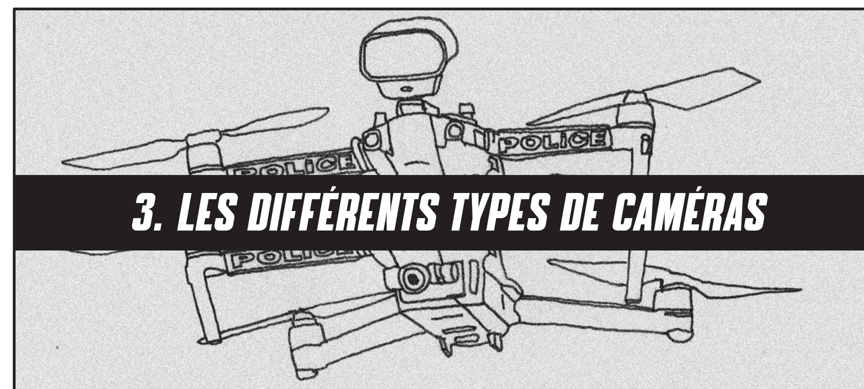
> *Dix mâts de vidéoprotection sciés cet été [2022]: à Nangis, la facture atteint près de 250 000 euros.*

La disqueuse sur batterie. Technique longue, onéreuse et bruyante, mais diablement efficace. Les saboteur-euse-s scient le mat, toute l'installation est à reconstruire.

Bélier

> *Il est un peu plus de minuit, dans la nuit du 8 au 9 janvier 2022, lorsque les forces de l'ordre sont appelées pour intervenir dans le quartier de la Gabelle, à Fréjus. Sur place, des individus utilisent une mini-pelleteuse pour fracturer une caméra de vidéosurveillance, placée devant la cité. D'autres tentent d'asperger l'objectif de peinture à l'aide de tirs de paintball. Ils mettent également le feu à l'engin de chantier et à un scooter.*

Foncer dans le mât avec un engin de chantier ou n'importe quel véhicule qui est en plus incendié au pied du mât, notamment si le bélier n'a pas fonctionné. Les urbanistes mettent souvent des barrières et des plots pour éviter ce genre d'attaque.



3. Les différents types de caméras

Il existe un très grand nombre de types de caméras de vidéosurveillance selon plusieurs caractéristiques : l'apparence, la résolution, la mobilité, les modes (infrarouge, thermique, ...), le champ de vision, le zoom, etc. On peut néanmoins différencier quelques grandes catégories de caméras.

• Les caméras directionnelles ou fixes

Elles surveillent un plan unique plus ou moins large, et peuvent avoir un zoom. Leur forme donne une indication sur l'endroit qu'elles surveillent. Elles sont souvent utilisées pour surveiller des points de passage obligé : un couloir, une entrée, etc.



• Les caméras mobiles PTZ (*pan tilt zoom*)

Elles peuvent pivoter à 360°, s'incliner de haut en bas jusqu'à 180° et possèdent des zooms optiques. En raison de leurs caractéristiques, celles-ci sont souvent utilisées pour surveiller des zones étendues.



• Les caméras dômes fixes et mobiles



La caméra dôme est une caméra installée à l'intérieur d'une demi-sphère en verre. Elle est beaucoup utilisée en raison de sa résistance au « vandalisme » et en raison du fait que la coupole ne permet pas souvent, à cause de son opacité, de voir où pointe l'objectif. Elle est vendue comme une caméra « discrète ». Cette caméra peut être fixe ou mobile (pivoter à 180° et s'incliner vers le haut et le bas).

• Les caméras panoramiques multi-capteurs

On parle de caméra multi-capteurs pour désigner une caméra qui possède plusieurs capteurs dans un seul boîtier et qui permet ainsi de réaliser une vue panoramique d'un certain angle (jusqu'à 360°) en mettant côte à côte les images des différents capteurs. On a ainsi plusieurs caméras (grâce aux différents capteurs) en une seule, ce qui est « avantageux » d'un point de vue technique – il n'y a qu'une seule caméra à installer – comme du point de vue de la surveillance – on a une vue panoramique. Ces caméras sont très utilisées dans les aéroports, les gares, les carrefours, les places, soit dans tous les espaces où une vue panoramique est utile.



La première image montre ainsi une caméra possédant quatre capteurs, qui permet de réaliser une vue à 180°. Ces caméras ont l'intérêt, au regard de leur fabriquant, de proposer une vue panoramique sans perdre en qualité d'image. En effet, contrairement aux caméras possédant un seul objectif grand angle, la caméra panoramique multi-capteurs permet de réaliser une vue panoramique d'une grande qualité.

Casser

*Durant les nuits du 28 au 31 août 2022, 7 des 15 caméras installées par la municipalité de Torcy, en Saône-et-Loire, ont été détruites. Les flics et le maire évoquent « des groupes de 2 à 6 jeunes adolescents », qui ont détruit les caméras « **au marteau et par jets de pierres** ». Les audacieux saboteurs ont même éclaté la caméra située sur le poste de police municipale. La facture s'élèverait à 50 000 €.*

Un bon vieux marteau fera souvent l'affaire si l'on arrive à avoir le globe à portée de main. Beaucoup aujourd'hui sont conçus pour résister aux attaques, avec du plexiglas plutôt que du verre. En s'acharnant un peu on finit quand même par en venir à bout et si la caméra résiste c'est souvent le support qui lâche. Parfois, sur les mâts, les constructeurs mettent des gaines anti-escalade, sorte de pics empêchant de monter au mât. Avec un peu d'adresse c'est aussi possible d'utiliser des projectiles.

*Vers 1 h 30, le 27 juillet 2022, les nantais-es ont entendu **six à sept détonations d'armes à feu** et un homme porteur d'une arme longue a, semble-t-il, été vu et une caméra a été détruite.*



9.1 S'ATTAQUER À LA CAMÉRA

Obstruer

Le 20 août 2020 à Portland (USA), lors d'une des nombreuses manifestations antiracistes et antipolice, le bâtiment de l'United States Immigration and Customs Enforcement (ICE, une agence de police douanière et de contrôle des frontières du département de la Sécurité intérieure des États-Unis) est tagué, ses vitres brisées et ***deux caméras sont aveuglées par des plots de chantier qui sont fixés dessus.***

Certain-e-s essayent de l'emballer dans un sac plastique, parfois avec une perche et un noeud coulant si elle est haute.

Peindre

Un coup d'aérosol sur l'objectif fera souvent l'affaire pour les rendre aveugles le temps d'agir. Très pratique pour les caméras de distributeurs de billets, ou les caméras à hauteur humaine en général. Pour celles moins accessibles, on a pu voir une caméra peinte avec un pinceau attaché à une perche.

Déplacer

Les directionnelles sont souvent déplaçables sur leur axe dans le but qu'elles regardent un mur ou le ciel plutôt que ce qu'elles visaient au départ. Encore une fois, si elles sont inaccessibles, un manche à balai pourra aider à les faire regarder ailleurs.

La deuxième montre une caméra ressemblant à un vaisseau spatial ou une soucoupe volante qu'on croise de plus en plus dans l'espace urbain. La partie supérieure de la caméra en forme de couronne possède entre quatre et huit capteurs permettant une vue panoramique à 360° d'une grande qualité. Mais en plus, elle possède une caméra PTZ (la demi-sphère sous la couronne), qui lui permet d'obtenir de « gros plans nets et détaillés, très utiles sur le plan judiciaire. »





La troisième présente un type de caméra très répandu à Paris. Les flics les appellent « Plater ». Avec ces caméras ressemblant à des « mamelles » ou à des « grappes », il s'agit aussi d'obtenir un plan panoramique à 360° grâce aux différentes caméras situées en haut, et d'avoir une caméra PTZ en dessous qui ici aussi permet de se concentrer sur un plan précis avec une plus grande qualité d'image.

• Les caméras nomades

Elles ont la particularité de pouvoir être déplacées très facilement. Leur type est variable et répond à des besoins spécifiques : caméra fixe, dôme, 360°, etc. Le plus souvent elles sont installées sur un lampadaire afin d'être reliées au circuit électrique de l'éclairage public. Elles sont équipées d'une batterie (boîtier blanc au-dessus du globe) qui se recharge la nuit lorsque l'éclairage est allumé. Le jour elle fonctionne en autonomie, grâce à l'électricité stockée dans la batterie. Elles disposent aussi d'un enregistreur et d'une solution de transmission sans fil qui peut être du wifi, de la 3G, 4G… Ces caméras répondent souvent à des besoins temporaires de surveillance dans un espace : « travaux importants nécessitant une surveillance, événementiel, problème de sécurité ponctuels dans une zone, dépôts sauvages, manifestation », etc.



• Les drones

Depuis quelques années, d'abord aux frontières, puis dans les rues lors de manifestations, ou encore pendant le premier confinement, un nouveau type de caméras de surveillance a fait son apparition, extrêmement mobiles et déployables rapidement en fonction des besoins des flics. Il s'agit des drones, ou « aéronefs circulant sans personne à bord » comme ils sont décrits par la loi. Même si leur usage a débuté bien avant qu'un cadre légal existe, l'État a récemment légiféré sur leur utilisation par les forces de l'ordre suite à une plainte de la Quadrature du net et de la Ligue des droits de l'homme. Une première tentative en 2021 dans la loi Sécurité Globale a été retoquée par le Conseil Constitutionnel. Quelques mois plus tard le package a été remis dans une autre loi, celle « sur la responsabilité pénale et la sécurité intérieure » ou drone 2, avec quelques modifications explicitant les conditions d'usage des drones, et promulguée cette fois-ci avec succès en janvier 2022.



Mis à part les policiers municipaux, les flics peuvent donc désormais officiellement utiliser les drones pour filmer à des horaires et des endroits précis sur autorisation préalable du préfet. La liste des situations où ils peuvent être utilisés est restreinte mais suffisamment floue pour s'appliquer n'importe où et n'importe quand : « la prévention des atteintes à la sécurité des personnes et des biens, la sécurité des rassemblements sur la voie publique, la prévention d'actes de terrorisme, la régulation des flux de transport, la surveillance des frontières, le secours aux personnes », et pour les nécessités d'une enquête ou d'une instruction portant sur les crimes et certains délits.

Les drones sont très discrets mais leur bruit est tout de même facilement reconnaissable, comme le bourdonnement d'un énorme essaim d'abeilles, pensons à regarder le ciel et faisons marcher notre imagination.



9. Esquiver et saboter les caméras

Lorsque l'État cherche à étendre son contrôle, à avoir des yeux omniprésents, nombreux-ses sont celles et ceux qui cherchent à s'y soustraire. Parfois contre la vidéosurveillance en elle-même, souvent pour pouvoir poursuivre leurs activités illégales.

Malgré l'étendue du maillage, il reste toujours des angles morts. Le site de cartographie collaborative openstreetmap permet d'afficher les caméras sur la voie publique qui ont été enregistrées par les utilisateur-ice-s (cf. encart p.81-83). Pourtant, il est quasiment impossible de ne jamais croiser les yeux automatisés des flics. Face à cela, il y a deux enjeux : ne pas être reconnaissable et ne pas être suivi-e.

Tromper la caméra peut être une question de temps, d'habits, de formes :

- Se changer dans un angle mort, ressortir avec une autre tenue quelques dizaines de minutes plus tard.
- Porter une casquette, un masque covid, un parapluie, des lunettes de soleil, des vêtements trop grands et difformes.
- Passer par des endroits avec de multiples sorties, varier les moyens de transport, prendre des chemins illogiques.

Pour lutter contre la surveillance, logiquement on en vient à réfléchir à comment rendre les caméras inefficaces. Voici quelques techniques de sabotages vues ces dernières années. Bien sûr, ce n'est ni objectif ni exhaustif, et c'est en essayant par soi-même qu'on est plus créatif-ve !

visionnent peuvent choisir quand iels jugent pertinent de garder des images, qui seront alors conservées dans le délai légal de 30 jours maximum.
Par ailleurs, les métros et trains de nouvelle génération ou rénovés sont dotés de matériel vidéo. Les images sont enregistrées sur disque dur et peuvent également être visualisées, selon le type de matériel, par le conducteur.

À la SNCF, l'usage et la sauvegarde des images est similaire au fonctionnement de la RATP. Il y a un PC national de sécurité et 5 centres de gestion des images en Île-de-France.

En juillet 2022, un CSU spécifique aux transports en commun en Île-de-France a été inauguré, le centre de coordination opérationnelle de sécurité (CCOS). Son but est de coordonner l'action des différents services de sécurité des opérateurs de transport et de l'État en s'appuyant sur les 125 000 caméras du réseau France Mobilités. Des locaux de 1000m² sont implantés sur l'Île de la Cité, au cœur de la préfecture de police, et il est actif 7j/7 et 24h/24. Le CCOS rassemble la sous-direction régionale de la police des transports (SDRPT), la gendarmerie nationale et les services internes de sécurité, c'est-à-dire la SUGE pour la SNCF et les GPSR pour la RATP, en coordination avec l'ensemble des services de la préfecture de police.



• Les caméras piétons et embarquées

On peut citer encore d'autres types de caméras ultra-mobiles. Par exemples celles qui équipent la poitrine des flics, dites « caméras-piétons », qu'ils peuvent allumer ou éteindre à leur guise d'un seul clic. Les enregistrements comprennent le son et l'image, sont conservés 6 mois, et peuvent aussi être transmis en direct au commissariat. Les caméras clignotent vert quand elles sont allumées et rouge quand elle enregistrent, il faut savoir aussi que ce n'est pas forcément les flics qui les portent qui les activent mais qu'elles peuvent être déclenchées à distance. Attention, le boitier enregistre jusqu'à 2 minutes avant son déclenchement et 2 minutes après la fin de l'enregistrement. Bien que jusque récemment peu répandues et de mauvaise qualité, en 2021 l'État a annoncé leur généralisation à toutes les brigades puis tous les agents (policiers et gendarmes) du pays. C'est l'entreprise Motorola qui a remporté le marché public, estimé à 15 millions d'euros et 30 000 appareils, pour agrandir et moderniser le stock. L'usage des caméras-piétons a également été étendu par des lois récentes aux garde-champêtres et aux contrôleurs des transports en commun, à titre d'expérimentation pour le moment.

Il est aussi prévu d'ici 2023 que chaque véhicule de police soit équipé d'une caméra dite « embarquée ». La loi Sécurité Globale a instauré en plus des essais de caméras frontales embarquées sur les trains, bus, etc, pour le moment uniquement dans le but d'analyser les éventuels accidents.



Quelle autorisation faut-il pour installer des caméras sur la voie publique ?

Pour installer des caméras publiques, les mairies doivent monter un dossier de demande d'autorisation. Ce dossier est ensuite analysé par une commission départementale de vidéoprotection présidée par un magistrat qui rend un avis favorable ou défavorable. Puis la décision finale revient au préfet qui choisit ou non de suivre l'avis de cette commission. Une fois validée l'autorisation est donnée pour 5 ans.

Il y a deux cas où ce n'est pas les mairies mais directement le préfet qui prescrit l'installation de caméras publiques. Dans le premier cas, celui de la « prévention au terrorisme », le préfet peut en effet prescrire l'installation de caméras. C'est souvent le cas aux abords des centrales nucléaires, des usines SEVESO, des châteaux d'eau, mais également dans les transports, ou les aéroports. Dans le second cas, le préfet, « s'il est informé de la tenue imminente d'une manifestation ou d'un rassemblement de grande ampleur présentant des risques particuliers d'atteinte à la sécurité des personnes et des biens », peut décider sans avis préalable de la commission départementale de vidéoprotection, de délivrer une autorisation provisoire d'installation de caméras pour une durée maximale de quatre mois. L'autorisation est censée ne plus être valable une fois la manifestation finie. En bref, dans le cas où c'est le préfet qui décide, on voit que l'installation de caméras peut être quasi immédiate.

le cadre opérationnel de la « police d'agglomération »[2]. Mais on ne sait pas quelles communes ont fait le choix de s'y rajouter.
Il ne s'agit pas là de mutualisation des caméras puisque les flux vidéos sont a priori centralisés dans les centres de commandement parisiens. À l'inverse, ce n'est pas sûr que les CSU de banlieue aient accès aux images de Paris.

En 2013, dans le cadre du PVPP, plus de 4600 agents étaient habilités à visionner les images. Ce nombre a augmenté, notamment depuis 2019, où plusieurs agents de la préfecture, les militaires de la Brigade de Sapeurs-Pompiers, ceux des armées exerçant au sein des salles d'information et de commandement de la préfecture de police dans le cadre du plan VIGIPIRATE, ainsi que la police, les douanes, la gendarmerie, sont destinataires des images et enregistrements, en fonction des évènements. Depuis 2022, certaines images de caméras à Paris peuvent être visionnées par les agents municipaux, dans des circonstances restreintes (protection des bâtiments publics, régulation du trafic routier, infractions aux règles de circulation).

Pour visionner toutes ces caméras, il y a 427 postes d'opérateurs, pour 50 murs d'images et 85 sites d'exploitation dont des postes de commandement installés dans chacun des vingt commissariats d'arrondissement de la capitale. Les images sont disponibles 24h/24, 7j/7.

Dans le cas du réseau propre à la RATP, il y a près de 20 000 caméras de vidéo embarquées dans les bus et les trams et près de 10 000 caméras dans le métro et le RER, qui sont consultables en temps réel dans les PC (postes de commandement) de sécurité de la RATP (mis en place dès 1995) et de la police. Les images sont conservées pendant 72h et récupérables dans ce temps uniquement sur réquisition du procureur de la République. On imagine que le choix du délai inférieur au délai légal de conservation est dû aux limites de l'infrastructure qui conserve les données pour un très grand nombre de caméras. Mais les agent-e-s de de la RATP qui les

2 Depuis 2009, nouvelle autorité de la préfecture de police de Paris sur les flics de Paris et des départements de la petite couronne dans la logique du « Grand Paris ».

Il est d'ailleurs prévu, d'ici 2026, d'augmenter le nombre de flics dédiés à la vidéo-verbalisation.
Les JO de 2024 vont servir de prétexte à l'installation de nouvelles caméras (cf. partie 2). Dans le cadre du PVPP, la mairie de Paris a prévu d'ici 2026 d'installer 320 nouvelles caméras, dont la moitié d'ici les JO et un tiers qui le seront aux abords des sites des JO. La préfecture de police promet elle 415 nouvelles caméras aux abords des sites olympiques et des voies automobiles réservées aux JO pour 2024. Concernant les 500 caméras annoncées par le ministre de l'intérieur, on ne sait pas si elles s'ajouteront à ces trop nombreuses installations.

Fin 2020, il y a au total 37800 caméras de la région Île-de-France, qui sont reliées aux différents CSU parisiens encadrés par le PVPP. Parmi ces caméras, il y a les caméras permanentes sur la voie publique dont certaines appartiennent à la ville (comme les 300 qui étaient auparavant dédiées à la vidéo-verbalisation et dont le délai de conservation des images est identique aux autres caméras) et d'autres à l'État. Des caméras nomades (cf. partie 3) sont aussi reliées à ce réseau : elles peuvent être rajoutées momentanément par la préfecture de police et récemment des caméras piétons. À cela, s'ajoutent les « images tiers », qui élargissent la couverture des caméras à d'autres zones ouvertes au public à travers 102 partenariats avec des entreprises privées et publiques. On trouve au sein de ce réseau des caméras de la RATP, des gares SNCF, du réseau francilien de la SNCF, du réseau trafic Gerfaut, du musée du Louvre, du Louvre Carrousel, du Palais des Congrès, du Parc des expositions de la Porte de Versailles, de Villepinte et du Bourget, du Parc des Princes, du Stade de France, des centres commerciaux d'Aéroville, du Forum des Halles, de Beaugrenelle, de Rosny 2, de Créteil Soleil, des 4 TEMPS ou du Printemps Haussman.
Le nombre de caméras interconnectées est aussi le résultat du renvoi d'images de certaines communes des trois départements de petite couronne, Seine-Saint-Denis, Val-de-Marne et Hauts-de-Seine vers le PVPP de la préfecture de police de Paris, pour être utilisées dans



4. LA QUALITÉ DES IMAGES

La vidéosurveillance augmente indéniablement les capacités de contrôle de l'autorité, mais dans quelle mesure apporte-t-elle une aide conséquente à celleux qui veulent nous espionner ? Encore faut-il que les images soient exploitables ! Il apparaît donc important de connaître les performances techniques des caméras, en terme de qualité d'images, tout en appréhendant leurs limites. Elles peuvent permettre de détecter une activité « anormale » et déclencher une intervention, mais toujours dans la limite de leur champ de vision. Elles peuvent aider à identifier des individu-e-s, mais toujours dans la limite de leur précision. Elles peuvent fournir des images en couleur le jour, mais généralement pas la nuit... Toutes ces limites ne cessent néanmoins d'être repoussées par les constructeurs, au gré des innovations technologiques.

4.1 QUELLE EST LA PRÉCISION DES CAMÉRAS DE VIDÉOSURVEILLANCE ?

Jusqu'à quelle distance une caméra, et donc les agents qui sont derrière les écrans, peuvent-ils nous voir ? Évidemment il y a autant de réponses à cette question que de types de caméras aux performances techniques propres. Néanmoins, les collectivités en France ont logiquement tendance à s'équiper avec du matériel de capacité similaire, suivant les mêmes offres du marché de la vidéosurveillance, et les mêmes avis d'experts. À partir de ces tendances générales, on peut apporter des éléments de réponses approximatifs à la question posée plus haut.

Quelques exemples de ville :

- **Nice** : les caméras panoramiques multicapteurs ont une résolution HD.
- **Strasbourg** : toutes les caméras de surveillance de la voie publique ont une définition full HD.
- **Poissy** : toutes les caméras sont en full HD.
- **Pau** : toutes les camétas (120 au total) sont panoramiques et combinent un dôme PTZ et quatre caméras fixes de 5 millions de pixels (20 millions de pixels au total.

La précision d'une caméra dépend principalement de deux données techniques :

- la résolution d'image, à savoir le nombre de pixels qui composent l'image
- le champ de vision, plus il est large moins l'image est précise

Comme pour les écrans de télés la course à la haute résolution est de rigueur chez les constructeurs, et les villes adaptent leurs équipements au fur et à mesure. Si le full HD (1920x1080 pixels), soit 2 millions de pixels, reste aujourd'hui la résolution la plus courante, de plus en plus de caméras de quatre, cinq voire huit millions de pixels sont installées pour filmer sur des plans larges. Les caméras panoramiques multicapteurs migrent en ce moment de



8. LA VIDÉOSURVEILLANCE EN RÉGION PARISIENNE

Dès 2009, le réseau de caméras de la ville de Paris a été encadré par le plan PVPP (plan de vidéoprotection pour paris) appelé aussi plan « 1000 Caméras ». Ce plan a permis de définir les emplacements des caméras, leurs fonctions, qui les visionne et le contrat avec l'entreprise qui les installe, mais aussi leur entretien, leur mise à niveau et un réseau dédié de 600km de fibre[1]. Il est sous la responsabilité de la préfecture de police de Paris, et inclu aussi le visionnage de certaines images de la RATP et de la SNCF.

Un deuxième plan, PVPP-2, adopté en 2015 (pour 6,3 millions d'euros) a été motivé en partie par l'attaque dans les locaux de Libération en 2013, où la vidéosurveillance a été mise en avant dans la recherche de l'auteur des faits.
Il comporte de nouvelles caméras, dont des caméras « mamelles » (cf. partie 3) et une présence accrue dans des quartiers réaménagés ou nouvellement aménagés, ce qui fait un total de 4171 caméras dans Paris (chiffre de la Quadrature du net). Ces nouveaux équipements feront du 1er arrondissement le plus vidéosurveillé de Paris avec une caméra pour 314 habitant-e-s. Un autre des arguments utilisés pour la mise en place de ce deuxième plan a été la lutte contre la pollution de l'air. Selon la mairie, les caméras permettraient de mieux contrôler les rues où la circulation est interdite ou réduite.

1 Contrat entre l'État et IRIS-PVPP, une filiale de GDF Suez, installée à Courbevoie (92) cofinancé par l'État et la mairie de Paris pour 5 million d'euros, pour une durée de 15 ans.

serait pas le cas, non sans par ailleurs ouvrir encore plus grand la porte à l'emploi de la VSA. Il n'y pas d'illusion à se faire cependant sur le fait que le gouvernement, les keufs et les industriels de la sécurité attendent impatiemment l'occasion propice pour relancer le débat. Il faut donc s'attendre à ce que dans les prochaines années ils retentent d'autoriser l'usage de la reconnaissance faciale dans des dispositifs de vidéosurveillance, sûrement en suivant le schéma classique des mesures sécuritaires : en l'employant d'abord dans un cadre limité qui rassurerait les citoyennistes tout en étant une première étape en vue d'une normalisation et d'une acceptation plus générale (comme essayé de le faire une députée en 2017 en proposant d'utiliser la reconnaissance faciale uniquement à partir d'une base de données des fiché-e-s S).

définition 12 Mégapixels (4 objectifs de 3 millions de pixels) vers des définitions de 20 ou 32 millions de pixels. Les caméras de type « vaisseaux spatiaux » comprenant 4 à 8 caméras fixes en couronne et une caméra PTZ motorisée au centre, migrent vers du 40 millions de pixels (5x8 millions). On parle ici des nouveaux standards pour des projets d'installation ou de rénovation, qui sont confrontés à des limites de coût et de stockage des données. Beaucoup de systèmes de vidéosurveillance sont encore majoritairement équipés de caméras full HD (2 millions de pixels), voire seulement HD (1280x720 pixels). Pour autant, les PTZ en full HD restent suffisamment précises pour lire des plaques d'immatriculation grâce à leur zoom.

À partir de la résolution d'une caméra on peut déterminer approximativement ses capacités à nous espionner lorsqu'il fait jour. Plus exactement, à l'aide de formules d'optique, on peut calculer des distances maximales au-delà desquelles les différentes missions de surveillance deviennent plus compliquées. Ces calculs doivent être effectués en trois étapes.

Etape 1 : connaitre la densité minimale de pixels nécessaire pour que les images soient exploitables

Cela s'appelle la résolution spatiale. Par exemple, si des flics veulent lire une plaque d'immatriculation, l'image de la plaque doit être composée d'un nombre minimum de pixels en-dessous duquel elle ne sera pas lisible. De la même manière, l'identification par reconnaissance faciale nécessite que l'image produite comprenne au moins 80 pixels entre les yeux du visage filmé. La résolution spatiale, ou densité de pixels, est exprimée en nombre de pixels d'une image pour chaque mètre dans la réalité. Le pôle judiciaire de la gendarmerie nationale précise sur son site internet des valeurs de résolution spatiale minimale à garantir selon différents niveaux de surveillance (cf. tableau ci-dessous).

On imagine bien que ces recommandations visent à pousser les collectivités vers de l'équipement toujours plus pointu. Il convient donc de se les représenter comme des exigences pour des conditions de vidéosurveillance optimales, et non comme des seuils en-dessous

desquels les différentes missions listées ne seraient plus réalisables. D'ailleurs d'autres recommandations sont bien moins exigeantes en la matière, comme celles établies en 2016 par le forum genevois de la sécurité (une association de professionnels du secteur).

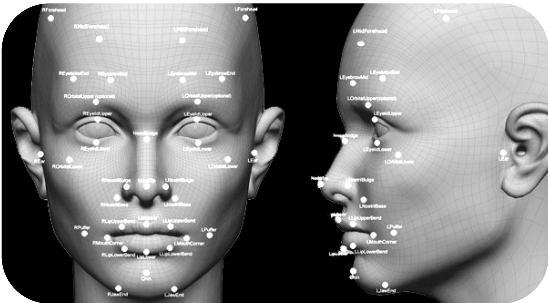
Pour se donner une idée approximative des capacités d'espionnage des autorités, mieux vaut se baser sur les exigences les plus basses en terme de résolution spatiale, correspondant à des conditions dans lesquelles le travail des flics ne serait pas idéal mais toujours possible. Alors on utilisera les chiffres du forum genevois.

Objectifs des flics lorsqu'ils visionnent les images transmises par les caméras	Résolution spatiale minimale recommandée	
	Par le forum genevois de la sécurité	Par le pôle judiciaire de la gendarmerie
Comprendre sommairement un évènement afin de déclencher ou non une intervention	Entre 1 et 30 pixels/mètre	30 pixels/mètre
Vérifier la matérialité d'un évènement ayant fait l'objet d'une alerte : différencier des individu-es entre eux, comprendre leur intéraction, voir dans quelle direction ils se déplacent, afin de déclencher ou non une intervention	30 pixels/mètre	100 pixels/mètre
Reconnaitre un-e individu-e ou un objet pour autant qu'il ait déjà été vu auparavant	50 pixels/mètre	/
Lire des plaques d'immatriculation	100 pixels/mètre	200 pixels/mètre

Etape 2 : estimer la largeur de champ maximale que la caméra peut filmer tout en conservant un niveau de densité de pixels donné

Il s'agit du champ de vision horizontal. Pour un nombre total de pixels donné, plus la densité de pixels nécessaire est importante, plus ce champ de vision risque d'être réduit. Pour le mesurer il faut

Et s'il était encore largement possible de refuser de se faire prendre en photo en garde à vue avant la loi d'avril 2022 – laquelle rend possible la prise d'empreintes et de photo de force si les chefs d'inculpation impliquent une peine d'au moins trois ans – il devient de plus en plus compliqué de le faire.



Pour ce qui est de l'association de la reconnaissance faciale avec des dispositifs de vidéosurveillance, c'est souvent à la fonction d'identification que ça touche. En théorie, un-e opérateur-ice habilité-e ou carrément un logiciel peuvent suivre une personne sur tous les réseaux de caméras d'une ville, à partir d'une photo extraite d'un fichier ou même d'une prise de vue d'une caméra (à condition qu'elle soit d'une qualité suffisante pour être exploitable). Plus les technologies d'identification évolueront et le maillage de caméras se renforcera, plus les flics seront capables de suivre avec précision les déplacements de n'importe quelle personne. Aujourd'hui la reconnaissance faciale en direct fait encore face à des barrières légales qui l'empêche d'être mise en application massivement et de manière indiscriminée dans les dispositifs de vidéosurveillance. Cela dit les capacités techniques existent et on n'est qu'à quelques décrets et quelques adaptations d'infrastructure de voir ce genre de dispositifs mis en place. A Nîmes par exemple, un adjoint au maire se vante même d'être « à un clic de la reconnaissance faciale » (le logiciel dont il dispose le permet déjà et il lui suffit de l'activer). Ces dernières années on a craint que les JO de 2024 soit le prétexte à l'implémentation ou l'expérimentation de la reconnaissance faciale dans l'espace public, le gouvernement a fini par annoncer que ce ne

antécédents judiciaires), autorisée depuis 2012, a été utilisée en moyenne plus de 1000 fois par jour en France en 2019 et plus de 1200 fois par jour en 2020. Ces chiffres représentent le nombre de tentatives de l'employer et pas forcément le nombre de fois où son usage a abouti à des résultats probants pour les flics (souvent la qualité insuffisante de l'image sur laquelle on cherche à identifier quelqu'un-e ou l'absence des personnes dans les fichiers sollicités font échouer les recours à la reconnaissance faciale).

La reconnaissance faciale peut avoir deux fonctions : une fonction d'authentification, qui sert à confirmer l'identité de quelqu'un-e en comparant une image de son visage à une autre déjà enregistrée dans un fichier (utiliser la reconnaissance faciale pour déverrouiller un smartphone par exemple), et une fonction d'identification, qui permet de reconnaître et suivre une personne sur plusieurs images sans forcément avoir son identité (chercher et/ou suivre une personne dans une foule).

Le gros de l'usage fait de la reconnaissance faciale en France jusqu'à maintenant concerne l'authentification. Plusieurs fichiers contiennent des photos servant à la reconnaissance faciale. Le plus important c'est le TES (titres électroniques sécurisés) qui contient les photos de cartes d'identité et passeports. Pour le moment il n'est censé servir qu'à vérifier que la personne contrôlée est bien celle sur la pièce d'identité. C'est un fichier qui est surtout utilisé aux contrôles aux frontières et qui légalement ne peut pas être consulté par les flics ou la justice pour d'autres affaires. En revanche le TAJ est aussi un fichier qui a recours à la reconnaissance faciale mais qui lui est largement utilisé par les flics. Ce fichier regroupe les infos des personnes ayant déjà eu affaire aux flics (en tant que gardé-e à vue, témoin ou victime) dont notamment des photos (en 2018 le fichier comprenait 19 millions de fiches et 8 millions de photographies de visages de gardé-e-s à vue). De là, les flics au moment d'un contrôle peuvent prendre une personne en photo et comparer au TAJ grâce à la reconnaissance faciale pour voir si une identité ressort, mais ils peuvent aussi essayer à partir d'un extrait de vidéosurveillance ou d'une image récupérée sur internet, sur un téléphone ou sur les réseaux sociaux dans le cadre d'une enquête.

appliquer la formule suivante :

Champ de vision horizontal (m) = 2 x Définition horizontale d'image (pixels)/résolution spatiale (pixels/mètre)

La définition horizontale d'image correspond au nombre de pixels maximum d'une image sur le plan horizontal. Par exemple la définition horizontale d'une image en full HD (1920x1080pixels) est de 1920 pixels. En HD (1280x720 pixels), elle est de 1280 pixels.

Etape 3 : Mesurer la distance maximale entre l'objectif et la cible à observer jusqu'à laquelle la précision de l'image est optimale pour une mission de surveillance donnée

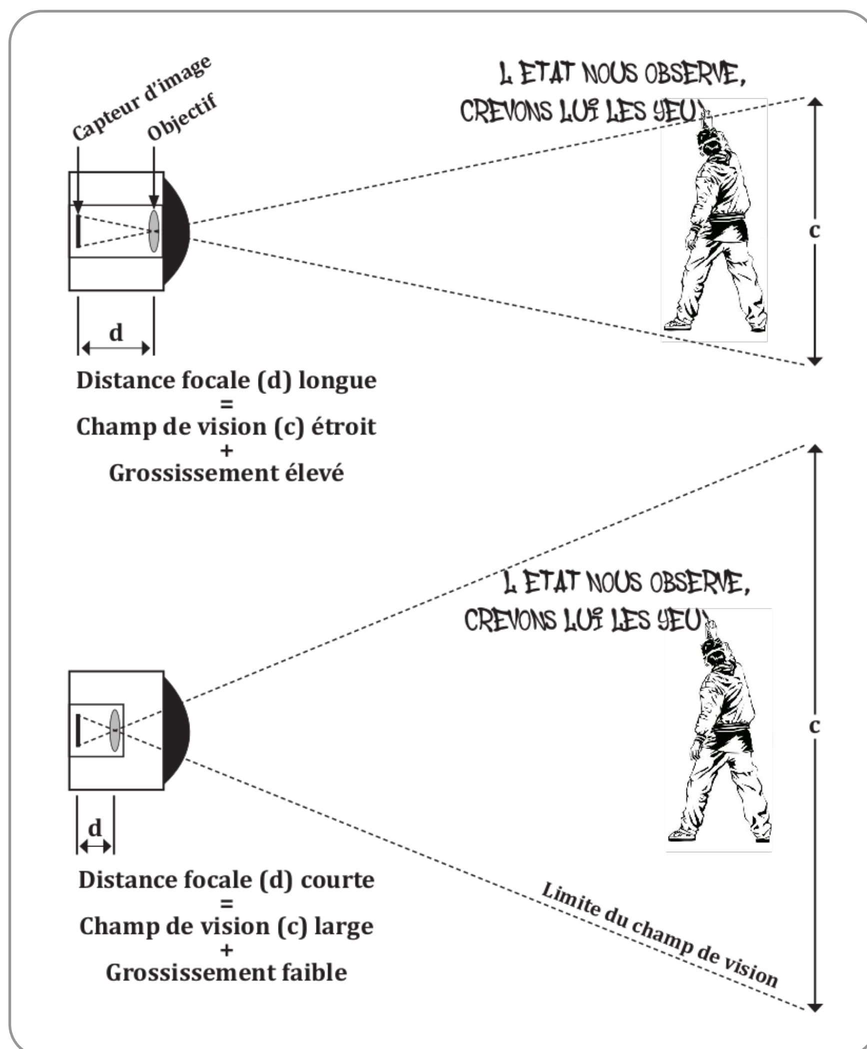
Pour mesurer cette distance on applique la formule suivante :

Distance (m) = distance focale (mm) x champ de vision horizontal (m) / taille du capteur d'image (mm)

Le capteur d'image, à l'intérieur de la caméra, est une surface photosensible de forme rectangulaire qui permet d'enregistrer l'image. Plus cette surface est grande, plus le champ de vision est large. Sa taille, pour des caméras de vidéosurveillance, varie de 6mm à 11mm de diagonale. Pour les calculs on prendra la valeur la plus haute (11mm), étant donné la nécessité de grands angles pour surveiller l'espace public.

La distance focale, ou focale, correspond à la distance entre le capteur d'image et l'objectif de la caméra (cf. schéma page suivante). Plus elle est réduite, plus le champ de vision est large, moins l'image est précise car les pixels sont plus dispersés, pour un nombre de pixels donné. Or, la focale des caméras de ville est souvent faible (environ 3mm) pour obtenir des plans larges sur un tronçon de rue, un carrefour ou une place. Néanmoins les caméras disposent de plus en plus d'une focale variable, ce qu'on appelle communément un zoom. En effet, des caméras comme les PTZ disposent d'un zoom permettant généralement d'augmenter la focale de 2,8mm à 12mm, mais des zooms plus puissants existent et se généralisent, certains pouvant augmenter la focale jusqu'à 43 fois.

Schéma de la focale



7.2. La reconnaissance faciale

Même si elle est vouée à y être associée la reconnaissance faciale n'est pas un système de vidéosurveillance automatisée. C'est un outil qui permet d'associer à chaque visage une « signature » unique en mesurant l'écart entre différents points choisis sur le visage et donc potentiellement reconnaître et/ou identifier ce dernier sur une image.

Partout la reconnaissance faciale s'impose comme un horizon inévitable des dispositifs de surveillance. Devenue un sujet de plus en plus présent ces dernières années, la technologie de la reconnaissance faciale fait beaucoup parler d'elle. Dans la masse d'informations sur le sujet il devient difficile de connaître ses usages et surtout ses capacités à un endroit et un moment donnés. D'autant que les acteurs sur le sujet ont souvent intérêt à exagérer ou minimiser son développement selon leur position (start-up qui cherche à vanter son produit ou agence publique qui tient à rassurer les citoyennistes soucieu-x-ses des libertés individuelles) et le contexte (réticences citoyennistes ou campagne de politique sécuritaire). Dans les discussions sur le sujet la Chine fait souvent office d'épouvantail d'un avenir possible : utilisation de la reconnaissance faciale dans les salles de classe ou dans les gares, base de données associant la photo et le score social des gens (qui conditionne ensuite l'accès à de nombreux services publics, droits sociaux et économiques), keufs dotés de lunettes capables de reconnaissance faciale. Cette panoplie dystopique fait évidemment froid dans le dos mais il ne faut pas oublier que sa puissance répressive repose aussi sur la peur qu'elle génère et que si on subira peut-être un jour le futur que nous promettent les mauvais films de science-fiction, pour le moment la reconnaissance faciale est toujours limitée par la technologie et l'infrastructure qui la supporte.

En France si son usage est encore limité on serait naïf-ve-s (et mal informé-e-s) de croire qu'on est épargné-e-s car la reconnaissance faciale est bel et bien là et les services de l'État et les boîtes privées ne s'en privent pas. Par exemple la reconnaissance faciale via les images des personnes fichées dans le fichier TAJ (traitement des

• DÉTECTEUR AUTOMATIQUE DE FRAUDE DANS LES TRANSPORTS

De mai à juillet 2022 à Besançon, deux lignes de bus Keolis ont été équipées de capteurs comprenant des caméras, et d'un logiciel permettant d'estimer le nombre de personnes qui fraudent. Le but affiché est de « lutter contre la fraude dans les transports en commun en s'appuyant sur la science comportementale ». Le logiciel compte les passager-ère-s monté-e-s à bord en même temps que le nombre de validations de titres de transport, puis effectue la soustraction avant d'afficher en temps réel sur un écran le nombre de personnes qui ont fraudé. En plus d'afficher en temps réel les potentiel-le-s fraudeur-euse-s, l'écran présente trois différents messages en fonction du niveau de validation : « Félicitations, vous êtes super » lorsque le nombre de fraudeurs-euse-s est très réduit, « Jouez le jeu » avec des avertissements paisibles quand le taux de fraude augmente, et, enfin, une alerte lorsque les fraudeurs-euse-s s'avèrent nombreux-ses. La boîte ayant conseillé Keolis pour la réalisation de cette technologie est NF Etudes. Elle se présente comme une agence de conseil, d'accompagnement et d'expérimentation en psychologie sociale et sciences comportementales ». Malgré l'affirmation de son concepteur selon laquelle ce « fraudomètre » vise « à inciter les individus à changer de comportement sans les contraindre », il permet de pouvoir faire des statistiques sur les lieux et horaires de fraude afin d'adapter les contrôles, voire même d'envoyer des patrouilles de contrôleurs en direct en cas de fraude massive.

Comment connaître la résolution et la focale d'une caméra dans la rue ?

Connaitre ces données techniques pour une caméra en particulier semble compliqué mais on peut tout de même obtenir certaines informations générales qui donnent des orientations.

Selon l'année d'installation on peut deviner quelle serait la résolution maximale d'une caméra. Une caméra installée avant 2019 a très probablement une résolution qui ne dépasse pas le full HD (1920x1080 pixels), d'après ce que disent les experts de l'AN2V (association nationale de la vidéoprotection) dans leurs guides Pixels.

Selon la forme on peut parfois distinguer les caméras PTZ, dont la focale est variable, des caméras dômes à focale fixe. Les PTZ sont souvent plus volumineuses et systématiquement suspendues à un bras horizontal. Lorsqu'il s'agit d'une caméra multi-capteurs, l'objectif central est probablement une PTZ avec un zoom, ou à minima une caméra mobile.

Selon la position de la caméra, lorsque sa focale est fixe, on peut deviner la valeur de cette dernière. Dans un espace étendu, comme une place ou un carrefour, la focale sera réduite, souvent proche de 3mm, pour avoir des plans larges. Dans une rue étroite le réglage de la focale sera à priori supérieur, pour optimiser la qualité d'image.

Selon la marque qui, dans certains cas, est imprimée ou indiquée avec un sticker sur la caméra, on peut retrouver des indications techniques, voire le modèle, en consultant le catalogue de produits sur internet.

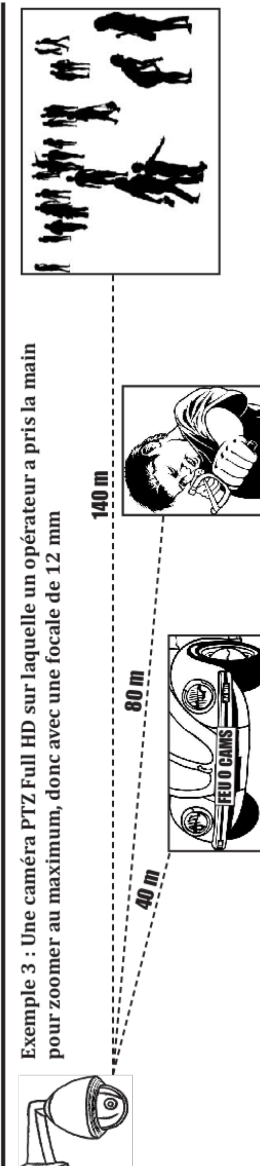
Trois exemples de caméras couramment utilisées

Pour chacune d'entre elles on peut donc estimer des distances au-delà desquelles l'exploitation des images n'est plus optimale.

d = *distance depuis l'objectif de la caméra jusque laquelle un opérateur pourrait, de façon optimale,* **(a)** *lire une plaque d'immatriculation,* **(b)** *voir les détails d'un-e individu-e,* **(c)** *comprendre les intéractions entre individu-es et voir leurs directions*







les émotions que ce soit d'un-e individu-e ou plus largement d'un groupe et de produire des signalements si celles-ci renvoient à des comportements « à risque » dans l'idée de « repérer des suspects potentiels avant qu'ils ne passent à l'acte ». Ce projet dystopique a finalement été abandonné pour des raisons techniques, les réseaux IP de la régie de transport n'étant pas suffisamment dimensionnés.

• Le renvoi d'image de téléphone par des volontaires (poukaves) vers des CSU.

Début 2018, la ville de Nice a expérimenté un dispositif permettant à des volontaires styles voisin-e-s vigilant-e-s, comité de quartier, agents municipaux, de renvoyer des images via leur téléphone au CSU afin de signaler des infractions, incivilités, etc. Reporty – application développée par la start up israélienne de l'ancien premier ministre Ehoud Barak – permet de partager des images en temps réel avec le CSU de la police municipale, qui géolocalise alors la position du smartphone et facilite l'intervention des keufs. En mars 2018, la CNIL a interdit l'usage de cette application, soulignant « le caractère disproportionné du dispositif avec ses risques d'atteintes à la vie privée » et mettant « en lumière les faiblesses des garanties sur ses mésusages ».

• Les caméras de dissuasion multimédia, avec son et lumière

S'il était déjà répandu, notamment à Cannet (06) depuis 2015 et à Hyères (83) depuis 2019, des caméras équipées de hauts-parleurs à travers lesquels les keufs pouvaient parler et réprimer les « incivilités » (tant pour dire à une personne de tenir son chien en laisse que pour signaler un stationnement illicite), sont actuellement conçues des caméras intelligentes qui repèrent *automatiquement* des comportements dits suspects par l'intelligence artificielle, que ce soit à travers la vidéo où à travers le micro. Ces caméras ont des micros, de l'intelligence artificielle, des flashs et des enceintes. Une fois le comportement détecté, la caméra peut par exemple envoyer des flashs en direction de la source de déclenchement tout en lui adressant un message. Par exemple, si le comportement détecté est un groupe faisant du bruit, le message automatiquement émis à travers le haut parleur sera « vous êtes dans une zone de vidéoprotection et les forces d'intervention sont en route ».

Si les logiciels que l'on vient de voir sont ceux actuellement utilisés dans certaines villes en France, voici une liste de ceux qui soit n'ont qu'été expérimentés et de ceux qui ont été formellement interdits après avoir été testés :

• La détection de port du masque

La ville de Cannes et la RATP à Paris ont utilisé ce genre de logiciel, proposé par l'entreprise Datakalab. À Cannes, entre avril et mai 2020, il s'agissait « d'évaluer le port du masque avant la sortie du confinement », dénombrant ainsi les personnes qui portent et ne portent pas de masque. Le logiciel a d'abord été utilisé dans trois marchés de la ville, puis dans les bus. À Paris, le logiciel a été utilisé durant trois mois à partir du 11 mai 2020 dans la station de Châtelet-les-Halles. Une douzaine de caméras ont ainsi eu pour but d'envoyer des SMS et mails à la RATP sur l'évolution du pourcentage de port du masque tout au long de la journée. Ces expérimentations ont finalement été « mises sur pause » par la CNIL. Bien que celle-ci estimait que le logiciel respecte les données personnelles par un système d'anonymisation, elle a finalement affirmé que « le dispositif ne permettait pas aux usager-ère-s d'exprimer leur consentement – faire non de la tête pour signifier leur refus – est insuffisant », invitant ainsi l'entreprise à réfléchir à une autre manière pour les usager-ère-s de montrer leur opposition.



• L'analyse d'émotions

En 2019, la ville de Nice a eu pour projet d'utiliser des logiciels de l'entreprise Two-i analysant les émotions des passager-ère-s du tram, prétendant détecter le stress, la sérénité, l'angoisse, la joie ou encore la déprime. Selon les mots mêmes de l'entreprise, « la cartographie émotionnelle en temps réel met en évidence des situations potentiellement problématiques voire dangereuses. Un déploiement dynamique des agents de sécurité dans une zone où la tension et le stress se font sentir, est souvent un moyen simple pour éviter tout débordement ». Autrement dit, il s'agirait d'analyser

Les calculs du schéma ci-contre sont théoriques et ne doivent pas effacer tout un éventail de possibilités, en particulier pour la reconnaissance ou l'identification d'un-e individu-e. Dans certains cas l'image peu précise d'une personne pourrait suffire à la reconnaitre car les flics du coin la connaissent déjà bien. Et puis, lorsque les images ne suffisent pas à elles seules, elles peuvent apporter différents niveaux de détails, de la couleur des cheveux à la marque des chaussures, qui, selon les cas, permettent d'aboutir à l'identification d'un-e individu-e, en complément d'autres sources d'informations (témoignages, etc...). Surtout, l'interprétation des images pour identifier une personne, ou déterminer ce qu'elle fait, demeure à l'appréciation des flics qui font l'enquête et des juges qui font le procès. Les flics peuvent affirmer identifier une personne en s'appuyant sur d'autres éléments d'enquête.

4.2 LES CAMÉRAS VOIENT-ELLES VRAIMENT DANS LA NUIT ?

L'une des premières difficultés de la vidéosurveillance est d'obtenir des images exploitables lorsque la luminosité est faible ou très forte (contre-jour). Or les équipements des collectivités sont souvent limités à des caméras de jour classiques, qui continuent de filmer en couleur la nuit à l'aide de l'éclairage public. Dans ce cas, la qualité des images est nettement réduite dès lors que l'obscurité s'installe. Du fait des mauvaises conditions de luminosité l'image est altérée par ce qu'on appelle le « bruit numérique », un ensemble de taches plus foncées ou plus claires, aussi appelées « pixels parasites », donnant un aspect granuleux à l'image.

Néanmoins, différentes technologies sont déployées pour optimiser la qualité d'image dans la pénombre et la nuit. Ainsi de nombreuses caméras sont désormais équipées du WDR (Wide Dynamic Range), qui permet de corriger simultanément les sous- et les sur-expositions. Pour se donner une idée, les dernières évolutions en matière de WDR atteignent des performances qui se rapprochent de celles de l'oeil humain en contre-jour et qui les dépassent nettement dans la pénombre. En revanche, le WDR permet seulement d'avoir des images en noir et blanc lorsqu'il fait nuit.

Pour filmer la nuit beaucoup de systèmes de vidéosurveillance sont équipés de caméras dites « jour/nuit ». Ces dernières disposent de LED infrarouges intégrées, généralement disposées autour du capteur d'images et produisant souvent une faible lueur rouge visible. De nuit, l'image est obtenue grâce aux réflections de la lumière infrarouge sur les personnes et les objets. Lorsque le jour se lève, un détecteur « de lumière visible » active la mise en place mécanique d'un filtre devant le capteur d'image. Ceci empêche la lumière infrarouge d'atteindre le capteur, afin de ne pas déformer les couleurs de la vidéo produites par la « lumière visible ». Le filtre s'enlève dès que la nuit retombe.

Si cette technique permet d'obtenir une image beaucoup plus nette la nuit, en supprimant l'effet du « bruit numérique », elle présente tout de même une limite de taille : l'image produite avec les LED infrarouges est en noir et blanc (niveaux de gris). Sans couleur, il est a priori plus difficile de reconnaitre les vêtements, le vélo ou la voiture d'un-e individu-e.

- **Le comptage.** Certains logiciels permettent de compter des personnes dans un espace et un temps donnés. Par exemple la SNCF expérimente ce type d'outil à Paris dans la gare RER « Bibliothèque François Mitterrand » et 11 gares du RER C, ainsi qu'en gare d'Antibes.

- **La détection de « maraudage ».** Il s'agit de logiciels capables de repérer des personnes qui restent au même endroit pendant un certain temps, et cela afin de traquer les pauvres qui occupent l'espace public. Ce dispositif a notamment été utilisé dans la ville de Suresnes (92). Dans ce sens, la RATP a expérimenté en 2017 un système qui détecte les personnes statiques pendant plus de 5 minutes. Les résultats ont par ailleurs été peu « probants » en raison de la détection récurrentes des « usagers qui attendent un rendez-vous ou qui cherchent simplement leur itinéraire ».

- **La détection de regroupement de foule.** Plusieurs villes en France possèdent des logiciels signalant automatiquement tout regroupement de foule.

- **La détection de colis suspects.** Les logiciels permettent de détecter des objets abandonnés dans les transports ou les lieux publics.

- **La détection d'armes.** La société française Two-i propose un logiciel qui comprend de nombreuses fonctions dont la reconnaissance d'armes.

- **La détection des distances sanitaires.** Two-i permet de calculer automatiquement les distances entre les individus qui sont dans le champ de vision des caméras. Cela lui permet d'analyser et de signaler le non-respect des distances sanitaires liées au covid 19.

- **La détection de « perte de verticalité »** permet de détecter des personnes qui chutent.

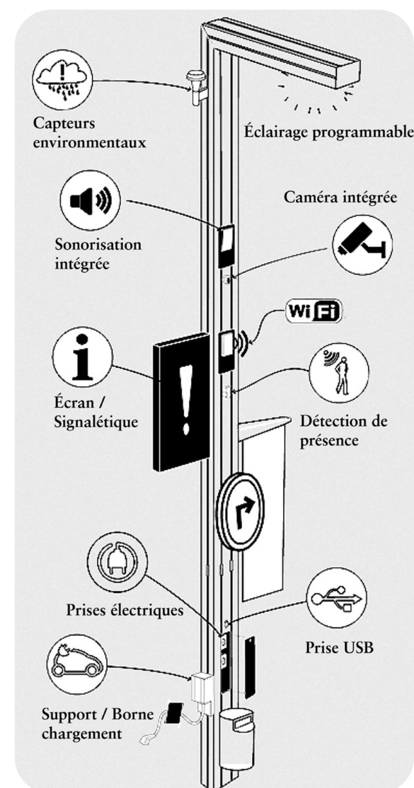
- **La détection d'incendie.**

- **La protection périmétrique.** Le logiciel repère toute intrusion dans un espace défini. Il peut tant s'agir de l'enceinte d'un établissement que des abords d'un distributeur de billet.



l'humain, une autre qui localise les membres sur ce corps humain, une autre qui repère les objets d'intérêt […] » pour ensuite envoyer une alerte sur le téléphone des employé-es du magasin. En bonus, Veesion se propose d'analyser « vos historiques de vol et [fournir] des recommandations personnalisées ». On sait que cette entreprise a vendu son logiciel à plus de 120 magasins en France dont des Monoprix, Franprix, Carrefour, Super U Express et Bio c'Bon.

• Les brumisateurs intelligents avec caméra intégrée



Il n'est pas ici question de vidéosurveillance automatisée à proprement parler, mais d'un exemple de « poteaux intelligents tout-en-un » exemplifiant le rêve actuel de la « smart city », soit de la ville ultraconnectée et bourrée de technologies comprenant de l'intelligence artificielle. Le brumisateur conçu par l'entreprise française Technilum, comprend ainsi, en plus de sa fonction rafraîchissante, « des caméras discrètes de vidéosurveillance à 180°, des capteurs de présence différenciée (piétons ou véhicules) pour faire varier l'éclairage ou lancer des alertes, des capteurs pollution et météo, des détecteurs de vibrations (en cas de tentative de vandalisme), des écrans interactifs, mais aussi des hauts-parleurs, des prises pour véhicules électriques et bien sûr internet (wi-fi et Li-fi) ». Technilum équipe de ces super-brumisateurs une ville située en périphérie de Cannes, Mandelieu-la-Napoule. Cette société propose par ailleurs tout une gamme de poteaux d'éclairage intelligents en plus de ces brumisateurs.

Trucs et astuces face aux caméras à LED infrarouges !

Des matières avec certaines propriétés réfléchissantes, de type vêtements brillants (ou bande réfléchissante de gilet jaune) peuvent parfois être représentées dans des teintes inattendues de niveaux de gris par les caméras à infrarouges. Par exemple, une veste noire d'une certaine matière peut apparaître dans une nuance bien plus claire et vice versa.

On pourrait aussi soi-même créer une surexposition d'infrarouges pour se rendre anonyme. Certain-e-s disent qu'en s'auto-éclairant avec des LED infrarouges disposées sur soi on crée, la nuit, une surexposition au niveau du capteur des caméras, comme lorsque l'on prend une photo en contre-jour. Par exemple une casquette équipée de LED infrarouges sur la visière permettrait d'empêcher les caméras de reconnaitre les visages pendant la nuit.

Si l'on n'est pas sûr que ce soit une caméra qui dispose de LED infrarouges, on peut le vérifier à l'aide d'un appareil photo. Les objectifs des appareils, comme ceux installés sur certains smartphones, sont capables de capter des longueurs d'onde plus importantes que celles du spectre visible, dont les infrarouges. Donc lorsque qu'on active un appareil photo devant un émetteur d'infrarouges, ces dernières apparaissent à l'écran.

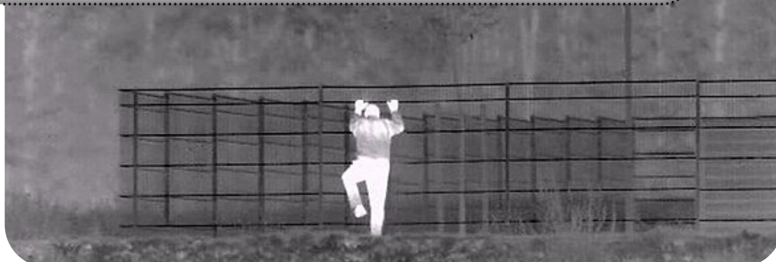
D'autre part, la portée de ce type de caméra est souvent assez limitée, la quantité de lumière infrarouge diffusée n'étant pas suffisante pour obtenir des images exploitables au-delà d'une distance de 30 à 40 mètres. Plus le nombre de LED est faible, plus la portée de la caméra est faible. Toutefois, pour augmenter la portée, des projecteurs infrarouges sont parfois installés à côté. Il s'agit d'une sorte de spot avec un écran blanc ou noir qui s'active automatiquement dès qu'il fait nuit. L'utilisation de ces LED puissantes à côté des caméras peut offrir une vision nette de loin mais à une très courte distance (quelques mètres) cela crée une surexposition, pouvant par exemple empêcher de voir le visage d'une personne.

D'autres caméras ont la capacité de surveiller des espaces la nuit : les caméras dites thermiques. En réalité ce sont des détecteurs de chaleur, qui sont sensibles au rayonnement infrarouge émis ou réfléchis par les corps et objets selon leur température, quelles que soient les conditions d'éclairage. Elles ne sont pas utilisées pour reconnaitre ou identifier des personnes, leur résolution étant faible (généralement 352x288 pixels ou 704x576 pixels), mais plutôt pour détecter une présence humaine dans des grands périmètres. On les trouve sur des sites militaires, des sites industriels sensibles de type Seveso, des sites d'OIV (opérateurs d'importance vitale) mais aussi sur les hélicoptères de la gendarmerie et au niveau de certains points de passage de frontières.

Des caméras thermiques pour le contrôle des frontières

Sur les plages du Nord-pas-de-Calais cela fait plusieurs années que les flics utilisent des caméras thermiques pour détecter la présence de migrant-e-s souhaitant traverser la Manche.

En 2021, l'État grec a installé des caméras thermiques sur l'ensemble de sa frontière avec la Turquie. L'Espagne compte faire de même à Mellila (enclave espagnole au Maroc) pour tenter d'empêcher les attaques régulières des trois clôtures de huit mètres de haut par des migrant-e-s souhaitant aller en Europe.



Exemple d'une caméra thermique avec vision en noir et blanc.

trois entreprises au moins ont l'air d'avoir été commercialisés et utilisés en France :



Anaveo, une entreprise de 320 personnes, travaille dans la vidéosurveillance pour la grande distribution. Son logiciel « SuspectTracker » promet de capter les flux d'images issus des caméras pour analyser les « comportements suspects », par exemple les « gestes vers poussette, sac à dos, poche de pantalon ou de veste ». Leurs présentations mentionnent en passant que la détection de vols vient alimenter une base de données permettant de continuer à améliorer l'algorithme. On ne sait exactement combien et quels magasins l'entreprise équipe, mais on sait qu'elle a au moins vendu son logiciel à un Carrefour Market à Bourges et à un Intermarché à Artenay.

Oxania, une start-up fondée en 2019, a produit un logiciel « Retail Solutions » qui serait capable de « reconnaître les gestes associés au vol en temps réel, détecter les comportements, les situations dangereuses, le parcours client et bien plus encore ». La vidéo de présentation assume calmement faire une analyse biométrique des comportements des personnes présentes dans le magasin : chaleur corporelle, gestes, corps,….

Veesion, start-up parisienne qui vend un produit de « reconnaissance des gestes » avec « une brique qui repère



• La reconnaissance sonore

Les logiciels permettent de détecter des bruits considérés comme suspects. Il s'agit par exemple de repérer « une signature sonore correspondant à une situation pouvant porter atteinte à la tranquillité publique, dans le cadre de la vie nocturne ». Grâce à une connexion au système de vidéosurveillance et son CSU, l'alerte donnée par le dispositif permet ensuite soit d'effectuer une levée de doute grâce aux caméras situées à proximité du capteur sonore, soit d'orienter automatiquement la caméra dans la « bonne direction ». Les signatures sonores correspondent souvent à des évènements de type cris, bris de verre, klaxon, alarme, spray de peinture.



Bien que cette technologie ait été interdite par la CNIL en 2019 à Saint Étienne suite à une mobilisation de collectifs locaux parce qu'elle consistait en un « traitement illicite de données à caractère personnel », celle-ci est largement utilisée en France. En effet, l'entreprise Sensivic affirme avoir signé un contrat avec le Ministère de l'Intérieur pour la « sécurisation » des JO 2024 et déployer ses dispositifs dans au moins 25 villes en France, principalement en région PACA et dans les Yvelines. La ville d'Orléans possède également ce type de capteurs qui continue d'être utilisé malgré des tentatives locales de s'y opposer. Il semblerait que l'entreprise justifie la légalité de ses technologies en affirmant qu'il est impossible de « remonter [à partir de ses capteurs sonores] à des voix, à des conversations, et qu'ainsi, aucune donnée pouvant être interprétée comme une donnée à caractère personnel n'est accessible ».

• La détection du vol dans les supermarchés

La VSA est également utilisée dans les supermarchés afin de faciliter la traque des « voleurs ». Ici le logiciel envoie un signalement lorsqu'il détecte un mouvement suspect pouvant être assimilé à du vol. Ces pratiques ne sont pas légales comme l'avait souligné la CNIL en 2020. Une fois de plus cela n'a pour autant pas mis fin à l'usage de ces techniques. Les produits de

4.3 Difficultés de maintenance et aléas techniques

Pour optimiser leur champ de vision et les protéger contre un coup de marteau bien senti les caméras sont très souvent installées en haut d'un lampadaire ou d'un mât, à environ 7 ou 8 mètres de hauteur. Mais cela présente plusieurs inconvénients pour leur bon fonctionnement, en particulier du fait des difficultés de maintenance induites. Au moindre souci technique il faut déplacer un camion nacelle et cela peut coûter cher ! D'où de nombreux cas de caméras qui fonctionnent moins bien car elles ne sont pas nettoyées ou réparées à temps.

Par exemple il arrive régulièrement que les caméras « jour/nuit » à LED infrarouges restent bloquées en mode jour ou en mode nuit du fait de la saleté qui obstrue le détecteur de lumière visible et maintient le filtre infrarouge activé ou désactivé. Si ce dernier reste activé en permanence, la caméra filme alors en noir et blanc de nuit comme de jour. S'il est maintenu désactivé les images produites la nuit sont bourrées de pixels parasites. L'accumulation de saleté sur les LED peut aussi largement altérer la qualité de l'image puisque l'éclairage infrarouge est en partie obstrué. Par ailleurs la chaleur des LED attire de nombreux insectes, en particulier les papillons, qui volent devant l'objectif.

En hauteur, le champ de vision des caméras se retrouve parfois masqué par des branches d'arbres, gênant l'exploitation des images en supplément des aléas climatiques, que ce soit la pluie, le brouillard, la neige et le soleil rasant.



Percher les caméras en haut d'un mât peut les protéger du vandalisme mais les expose à un autre obstacle, certes mineur mais toutefois intéressant à relever : la dégradation de la qualité des images du fait des oscillations du poteau. Plus la caméra est haute, plus l'image est soumise aux oscillations du mât. Une bonne brise contribuerait donc à notre anonymat !? En tout cas les caméras thermiques sont

particulièrement sensibles aux oscillations, les logiciels de traitement des images ne tolérant pas un écart supérieur à environ 0.015mm entre chaque point de l'image transmise.

Durée de vie des caméras

Si la plupart des caméras sont conçues pour fonctionner de façon optimale pendant au moins cinq ans, la durée de vie des LED infrarouges n'est parfois que de 20 000 heures, soit seulement deux ans d'utilisation si elles restent allumées en permanence, de nuit comme de jour. Remplacer les LED tous les deux ans semble une opération de maintenance compliquée et coûteuse, possiblement pas assurée de façon régulière.

Cette société propose ce type de logiciel mais également de la reconnaissance faciale. Il ne faut par ailleurs qu'une modification de paramétrage du logiciel de Briefcam pour ne plus reconnaître seulement le sens de déplacement et les vêtements d'un individu mais aussi son visage. D'un point de vue technique, dans les villes où ce logiciel est utilisé, on est donc à un « clic » de la reconnaissance faciale.

L'entreprise française Two-i basée à Metz propose également ce type de logiciel permettant de faire des recherches dans un historique de vidéosurveillance.

• L'analyse prédictive

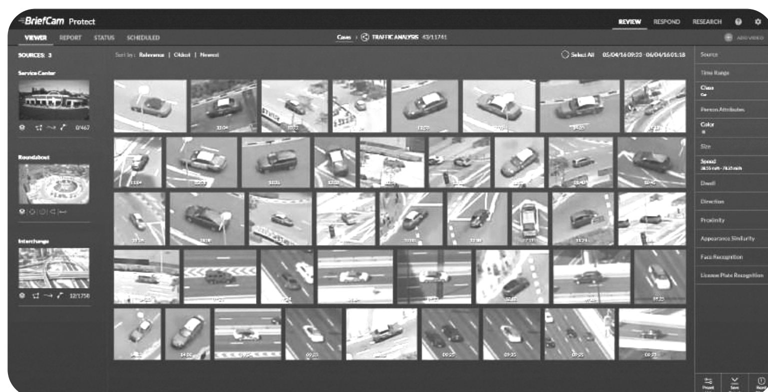
Le logiciel Map revelation de la société angevine Sûreté globale fournit des analyses prédictives, graphiques et géographiques sur des faits de « délinquance, incidents, ventes, évènements… ». Le logiciel est censé prédire, à l'aide d'un algorithme, les futurs crimes ou délits à partir des données récoltées par les keufs. L'idée étant de pouvoir, grâce à ces prédictions, mieux orienter l'activité des condés. Il y aura ainsi par exemple plus de patrouilles de keufs à tel horaire à tel endroit car les statistiques passées montre qu'il est probable qu'il s'y produise quelque chose. Ne constituant pas de la VSA à proprement dit, le logiciel est néanmoins conçu de sorte à pouvoir intégrer différents types de capteurs dont la vidéosurveillance et les alarmes au sein de ses cartes et interfaces. À Montpellier, la base de données provient à la fois de la police nationale (« vols de véhicule, cambriolages, vols à main armée...») et de la ville (« enquêtes de victimisation, interventions des services sociaux, remontées des bailleurs sociaux, ...»). Les villes de Montauban, Colombes, Lille, Angers, Villeurbanne, Lyon et Montpellier ainsi que des « collectivités » telles que la Gendarmerie nationale, la préfecture de police de Paris, la police aux frontières, possèdent ce genre de logiciel.





• La recherche et l'extraction d'images dans un historique de vidéosurveillance à partir de mots clés

Imaginons, des vitrines ont été brisées devant des caméras par un individu habillé en bleu. Grâce à ce module de vidéosurveillance automatisée, les keufs peuvent faire une recherche dans l'historique des caméras se trouvant à proximité. Ils vont taper les mots-clés correspondants (taille, genre, couleur des habits, vitesse de déplacement) et le logiciel va alors tenter de filtrer toutes les images et présenter toutes celles comprenant des individus habillés en bleu. Ils pourront ainsi, s'il y a suffisamment de caméras, plus facilement repérer le chemin de l'individu pour l'identifier.

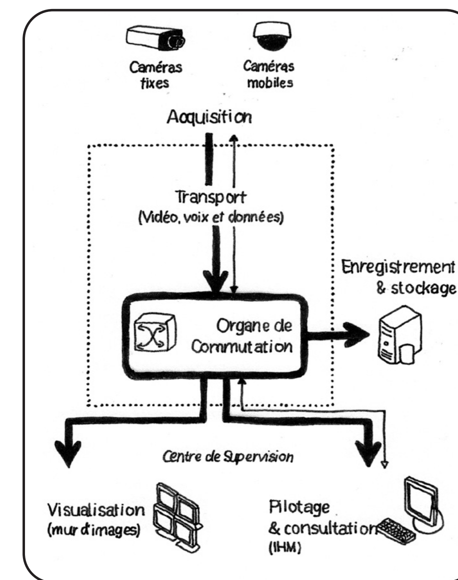


C'est par exemple ce que propose la société israélienne Briefcam qui, alors qu'elle n'équipait que 35 villes françaises en 2020 (Nîmes, Nice, Aix-Les Bain, Vannes, Deauville, Woippy, Roubaix, La Baule-Escoublac, Gex, Vaulx-en-Velin, Vienne, Moirans, Caveirac, Vitrolles) en équiperait pas moins de 200 en 2023. La SNCF utilise ce logiciel à Paris et Marseille. En 2019 à Nîmes, le logiciel de reconnaissance de forme aurait servi pour 1085 requêtes d'images dans le cadre d'enquêtes ! (Un article sur lequel nous sommes tombé-e-s affirme que la préfecture de police de Paris posséderait le logiciel de reconnaissance de forme de la société Briefcam. C'est le seul endroit où nous avons vu cette information, elle reste donc à confirmer.)



5. Le centre de supervision urbain (CSU)

La plupart des systèmes de vidéosurveillance publics possèdent un centre de supervision urbain (CSU) auquel sont transmises les images de chaque caméra (cf. encart p.38). Il existe quelques cas où les villes n'en ont pas. Dans ces cas là, il s'agit soit des projets de vidéosurveillance uniquement dédiés à la recherche a posteriori dans le cadre d'affaires judiciaires, sans suivi en direct, soit des villes où les images peuvent être directement consultées au commissariat. Au delà de ce dernier cas, la surveillance en direct passe le plus souvent par le centre de surveillance urbain. Ces fonctionnements ne sont pas unifiés au niveau national et il vaut donc la peine de se renseigner sur le fonctionnement de sa ville, qui est potentiellement spécifique. Dans cette partie nous allons détailler comment le CSU fonctionne : qui regarde les caméras ? Comment ? Avec quel matériel ? Et dans quel but ?



Transmission des images des caméras aux CSU

Ces dernières années les caméras numériques (caméras « IP »), utilisant internet pour transmettre les images, ont peu à peu remplacé les caméras analogiques, qui utilisent des câbles coaxiaux ou des ondes radio (réseau RLAN : bandes de fréquence 2,4GHz et/ou 5GHz). Dans les grandes villes les caméras IP sont souvent branchées au réseau de fibre optique qui permet le transport de grandes quantités de données vidéo jusqu'aux postes de visionnage et lieux de stockage. Dans les quartiers et communes où il n'y a pas de fibre optique les caméras IP sont mises en réseau à l'aide de câbles Ethernet, ou par des moyens sans fil tels que le WIFI ou les réseaux 3G/4G/5G. Par exemple, à Nice les images sont transmises via la fibre, et par ondes radio dans les zones où elle n'a pas été installée. À Strasbourg, la transmission des données se fait par câble Ethernet lorsque la fibre n'est pas présente. Si les moyens de transmission sans fil ont l'avantage de réduire les risques de sabotage de câbles et de faciliter l'installation des caméras, ils sont plus limités en flux de données et ouvrent la porte à d'autres types de sabotage. Depuis quelques années les installateurs vantent les mérites de la 5G qui pourrait partiellement résoudre ce problème avec un débit 14 fois supérieur à la 4G. L'optimisation de la vidéosurveillance est même un des arguments avancés pour le déploiement du réseau 5G.



Exemple d'un message d'alerte

INFORMATIONS : délit de fuite.

INFORMATION SUR LA SURVEILLANCE : surveillance dans un cadre judiciaire.

CONDUITE À TENIR :

- *Véhicule mis en surveillance sur l'ensemble du territoire national. Véhicule avec occupant.*
- *Signaler la présence ou le passage et identifier discrètement les occupants.*
- *Ne pas interpeller les occupants pour d'autres raisons que celles ayant motivé le contrôle sauf si ces personnes font l'objet de recherches actives au FPR.*
- *Aviser téléphoniquement le service ayant demandé la mise sous surveillance et confirmer par rapport.*
- *Assurer une surveillance discrète en vue de l'identification des utilisateurs.*
- *Solliciter sans délai les instructions du service ayant demandé la mise sous surveillance.*

En 2020, dans le cadre d'une enquête autour d'un incendie d'antennes relais, les flics ont été chercher les plaques enregistrées durant la nuit par un LAPI d'une boîte de sécurité privée dans un village à une vingtaine de kilomètres du lieu de l'incendie. On ne connaît pas la légalité de ce dispositif, mais il montre que des privés peuvent posséder de tels lecteurs et que les flics n'hésitent pas à s'en servir.



Les caméras qui font de la LAPI ressemblent soit à des caméras directionnelles, soit à des sortes de boîtiers. Dans le dernier exemple les lumières sur le côté correspondent à l'infrarouge nécessaire à ces caméras pour fonctionner de jour comme de nuit. Mais en plus de ces caméras que l'on peut trouver dans l'espace urbain, les gendarmes, les polices nationale et municipale possèdent des véhicules comportant, à l'intérieur de l'habitacle et des gyrophares, des caméras LAPI. Le dispositif fonctionne de la manière suivante : il suffit au véhicule de rouler pour que les caméras lisent automatiquement toutes les plaques d'immatriculation qu'elles ont dans leur visu. Si une plaque est comprise dans les fichiers FOVeS et SIS, elle produit alors un message d'alerte comprenant les raisons du signalement ainsi que la conduite à tenir.





5.1 LES OPÉRATEUR-RICE-S DU CSU

Tout CSU possède une personne responsable du système d'un point de vue juridique. Dans le cadre de la vidéosurveillance publique, c'est presque toujours le-la maire de la ville. Il est assez facile de savoir qui est exactement cette personne en allant consulter les bulletins d'information administratifs des villes et ainsi possible de leur mettre la pression d'une manière ou d'une autre. Concernant les autres personnes ou entreprises impliquées dans la maintenance, l'installation ou dans la communication du système, il faut faire plus de recherches et les informations ne sont pas toujours accessibles. Ensuite le CSU possède des « opérateur-rice-s ». Ce sont les personnes en charge de surveiller les images des caméras et de faire des signalements. Iels signalent tant un incendie qu'une « atteinte aux biens » en passant par de la gestion de la circulation et de la vidéoverbalisation.

Trois choses nous semblent mériter un peu d'attention concernant les opérateur-rice-s. La première concerne la question juridique de qui peut surveiller la voie publique. Il est aujourd'hui illégal de confier la surveillance de la voie publique à un personnel mis à disposition par une entreprise privée ou de renvoyer pour exploitation des images publiques à une entreprise privée. Autrement dit, c'est toujours la commune qui doit recruter ces opérateur-rice-s. De fait, les communes doivent prévoir le recrutement d'agents municipaux ou confier ce travail à des agents déjà en poste. C'est pourquoi la majorité des larbins des CSU sont des flics municipaux et des ASVP (agent sécurité voie publique). Par ailleurs, l'installation de systèmes de vidéosurveillance dans les villes a très souvent été accompagnée de la création d'une police municipale – dans ce cas, le CSU se trouve souvent dans les locaux de cette dernière. On notera aussi qu'il n'existe pas, pour l'instant, de formation commune d'opérateur-rice de vidéosurveillance en France.

Le second point concerne le rapport entre le nombre de caméras et le nombre d'opérateur-rice-s. On peut dire qu'il y a globalement toujours trop de caméras et pas assez d'opérateur-rice-s pour les surveiller. Les acteurs-trices de la vidéosurveillance disent qu'un-e agent-e ne peut surveiller efficacement qu'entre cinq et huit écrans

simultanément. Si on prend l'exemple du CSU de Nice, qui est le plus grand de France, on voit que les opérateur-rice-s sont forcément en sous effectif : puisqu'il y a 2510 caméras, il faudrait qu'il y ait constamment entre 314 et 592 opérateur-rice-s 24h/24 pour que le parc de caméras soit « constamment et efficacement surveillé » – ce qui n'est pas le cas, seule une centaine d' opérateur-rice-s y travaillent, autrement dit, il n'y en a en temps normal pas plus. A Paris, selon des chiffres de 2020, on compte 427 poste d'opérateur-rice pour 4000 caméras. Il en va de même dans les plus petites villes : par exemple à Poissy (39 000 habitant-e-s), il n'y a que trois écrans de surveillance pour 80 caméras et sept opérateur-rice-s pour une surveillance 7j/7 et 24h/24. Ici les opérateur-rice-s ont ainsi entre trois et cinq fois trop de caméras à regarder pour être « efficaces ». On sait aussi que beaucoup de CSU de petites villes n'ont pas de surveillance de nuit, avec des exceptions certains jours comme le 31 décembre. D'autres ont des effectifs réduits la nuit – ce qui diminue encore la possibilité, déjà peu élevée de jour, de faire de la flagrance durant ces horaires. Les images peuvent aussi être transmises au commissariat pendant la nuit. Il n'y a pas de règles concernant les horaires et les jours de la surveillance.

Le troisième point concerne le travail type d'un-e opérateur-rice. Selon une étude, les opérateur-rice-s réalisent un certain nombre d'opérations durant leur temps de travail. Tout d'abord, iels opèrent des rondes de surveillance passive : il s'agit d'effectuer un balayage rapide de toutes les caméras afin de repérer une éventuelle anormalité ou un problème technique. Ensuite, iels effectuent de la surveillance active : il s'agit ici de chercher activement le flagrant délit. Les opérateur-rice-s se concentrent souvent sur des caméras montrant des zones considérées comme « à risque » et sur des individus également considérés comme tels (évidemment les pauvres, les personnes racisées, les jeunes, les groupes, les gens qui courent, etc). Aussi, dans la plupart des CSU, les opérateur-rice-s doivent prendre en note leurs activités et des informations que leur transmettent les keufs – chose qui occupe une part non négligeable de leur temps. Pour finir, les opérateur-rice-s passent une large part de leur temps à ne pas faire de surveillance : que ce soit en faisant des pauses ou en regardant

On liste ici des logiciels dont on est sûr-e qu'ils sont actuellement utilisés dans certaines villes en France :

• La lecture automatique des plaques d'immatriculation (LAPI).

Il s'agit d'une technologie permettant d'identifier les plaques d'immatriculation des véhicules grâce à une technique de reconnaissance optique de caractères. Pour filmer les plaques de nuit, les caméras émettent de la lumière infrarouge. Le logiciel lit automatiquement les plaques et envoie un signalement s'il détecte un numéro de plaque figurant dans une base de données prédéfinie. La LAPI permet ainsi de générer une alerte lorsqu'un rapprochement positif est effectué entre la plaque d'immatriculation et ces fichiers. Les caméras captent et stockent une image de la plaque d'immatriculation et une image du véhicule, en même temps que la date, l'heure et la géolocalisation de chaque véhicule photographié, puis transmettent l'information aux services de police. Lorsque le véhicule n'est pas rapproché avec les fichiers, ces informations et photographies sont conservées au maximum huit jours ; si le rapprochement est positif avec les fichiers, elles peuvent être conservées pendant un mois.

La base de donnée en France à partir de laquelle se fait la comparaison et le signalement est celle des fichiers FOVeS (fichier des objets et véhicules volés et signalés) et SIS (système d'information Schengen). Le SIS comprend les personnes recherchées en vue d'une arrestation ou d'une extradition, les personnes disparues, certaines personnes interdites de séjour et les objets recherchés en vue d'une saisie ou dans le cadre d'une procédure pénale. En France il est notamment alimenté par le FPR (le fichier des personnes recherchées) lequel comprend tant les personnes recherchées pour des mandats d'arrêt, celles faisant l'objet d'une interdiction de conduire ou d'un contrôle judiciaire, que les personnes signalées comme dangereuses pour la sûreté de l'État (les fameuses fiches S). On n'est pas sûr-e et on a pour l'instant aucun exemple de cela mais il semblerait donc possible que la LAPI permette de signaler aux forces de l'ordre la présence et donc les mouvements des personnes fichées S (si le véhicule de la personne fichée S est lié au fichier).



La plupart des logiciels intelligents peuvent être ajoutés à n'importe quel parc de caméras existant : il n'y a pas besoin d'avoir un certain type de caméra ou d'infrastructure, il suffit d'ajouter le logiciel dans l'interface de vidéosurveillance.

Jusqu'à la loi JOP2 (cf. partie 2), il n'existait pas de texte de loi spécifique encadrant la vidéosurveillance automatisée. Pour autant son déploiement n'était pas interdit. Dans un avis de juillet 2022, la CNIL a opéré ainsi une distinction entre des usages « légitimes » et « illégitimes ». Légitimes seraient les usages à des fins statistiques à condition que les résultats soient anonymes. Par exemple : « Un dispositif permettant de calculer l'affluence dans un métro pour afficher aux voyageurs les rames les moins remplies vers lesquelles se diriger ». Illégitimes seraient ceux qui ont pour objectifs de détecter et de poursuivre des infractions. Par exemple : un algorithme repérant les destructions de mobilier urbain comme c'est le cas à Marseille. Aussi elle a rappelé que dans tous les cas, la réglementation sur la protection des données inclut un droit de s'opposer aux traitements algorithmiques, lequel n'est absolument pas appliqué et applicable de manière générale. On aurait pu penser que cet avis de la CNIL ouvrait la voie à l'interdiction de ces technologies - qui on le sait sont déjà utilisées dans leurs usages « légitimes » comme « illégitimes » dans au moins une cinquantaine de villes en France. Mais il n'en est évidemment rien, au contraire, la CNIL appelle à construire prochainement un nouveau cadre légal pour la VSA. La loi JOP2 en est la première étape. Autrement dit, bien loin de s'atteler à faire interdire des usages non conformes aux lois en vigueur, la CNIL semble vouloir embrayer leur légalisation.

les images autrement que pour les surveiller (une étude parle d'un opérateur ne cessant de regarder sa caisse pour vérifier qu'elle n'a pas été « vandalisée » ou volée ou d'un autre opérateur passant du temps à mater et commenter l'apparence de « femmes »). Aussi, tous les documents traitant du métier d'opérateur-rice ne cessent d'insister sur le fait que c'est un métier de merde où l'ennui règne et où il y a beaucoup de turn over. Difficile de prendre en compte cette donnée dans nos activités mais cela nous rassurera peut-être en nous rappelant que malgré tous les déploiements techniques impressionnants, le facteur humain peut faire tout foirer. De ce point de vue, cette étude (qui date de 2010) affirme que durant les 120h durant lesquelles les « ethnologues » ont assisté au travail des opérateur-rice-s, il n'y a eu « aucune identification sur le fait d'un délinquant, ni même a posteriori ». Si on peut nuancer aujourd'hui comparé à 2010 la rareté des flagrants délits dans le travail d'un-e opérateur-rice, ces dernier-ère-s n'ont pour autant toujours pas la capacité de scruter tout ce qu'il se passe sur les images qu'iels ont à surveiller. On verra plus loin que tout l'enjeu de la vidéosurveillance automatisée est ainsi de pouvoir augmenter l'efficacité de cette surveillance.

5.2 LES LOCAUX DE SUPERVISION



Tout poste de supervision est composé de plusieurs choses : un PC équipé d'une « interface homme machine » ; deux écrans : un écran pour l'interface graphique (souvent une carte avec toutes les caméras de vidéosurveillance) et un écran pour la visualisation des images ; un joystick de pilotage des caméras mobiles ; des moyens de communication pour contacter les dits services d'intervention (keufs, pompiers, etc). À partir de ces éléments de base, chaque CSU est organisé de manière particulière en fonction de sa taille et de ses objectifs de surveillance.

Reprenons l'exemple du CSU de Nice, qui rappelons-le est à « l'avant-garde » de la vidéosurveillance, pour voir une manière particulière de fonctionner et d'agencer un centre de supervision. En 2020, le CSU transmet les images de 2510 caméras. Il fonctionne 7j/7 et 24h/24. Il se trouve dans les locaux de la police municipale. Une centaine d'opérateur-rice-s y travaille. D'un point de vue matériel, le CSU comporte trois salles pour un total de 90 écrans. La première salle gère les évènements liés à la voie publique. Il s'agit de prévenir « les atteintes aux personnes et aux biens » en flagrance. Les images peuvent être renvoyées en direct « à la police nationale, à la police aux frontières, à la gendarmerie ». La police municipale se vante d'avoir permis 4227 interpellations grâce au CSU en un peu moins de neuf ans, ce qui donne un peu plus d'une interpellation par jour. Cette salle gère aussi « la prévention aux risques naturels ou technologiques, les secours aux personnes et la défense contre les incendies. » La deuxième salle gère « la protection des établissements scolaires et les transports (tramway, bus) », sachant que le tram comporte 900 caméras et qu'il y a une caméra devant chaque établissement scolaire. La troisième salle est dédiée à la vidéoverbalisation et à la gestion de la circulation. En plus des caméras, le CSU de Nice est relié aux alarmes des bâtiments publics et a un système permettant à des voisin-e-s/commerçant-e-s poukaves-vigilant-e-s formé-e-s par la police municipale d'envoyer des SMS de signalement.



7. LA VIDÉOSURVEILLANCE AUTOMATISÉE (VSA)

7.1. LES DIFFÉRENTS LOGICIELS DE VIDÉOSURVEILLANCE AUTOMATISÉE

La vidéosurveillance automatisée ou algorithmique (VSA), aussi appelée vidéosurveillance augmentée ou intelligente par ceux qui la promeuvent, est présentée comme l'avenir du secteur. Tous-tes les acteur-rice-s sont d'accord pour affirmer que l'augmentation du nombre de caméras, qui est la tendance actuelle, doit s'accompagner de vidéosurveillance automatisée. Car si le nombre de caméras augmente, le nombre d'opérateur-rice-s n'augmente pas aussi vite. Comme on l'a vu, les opérateur-rice-s ne sont jamais assez nombreux-ses pour surveiller toutes les caméras en direct, et encore moins de façon efficace. Sans VSA, l'augmentation du nombre de caméras par opérateur-rice-s diminue la qualité de la surveillance.

Il s'agit donc, avec la VSA et ses logiciels automatisés, de faire en sorte que toutes les images des caméras soient analysées en fonction de certains critères, et d'envoyer des signalements aux opérateur-rice-s, qui elleux traitent ensuite la validité des signalements. Autrement dit, la VSA permet d'augmenter le nombre de caméras sans déborder les opérateur-rice-s par un flux d'images trop important.

En raison de cette importance, de plus en plus de logiciels sont proposés par les entreprises. Il s'agit de l'ajout d'une couche d'algorithmes aux caméras de vidéosurveillance dites « classiques ». Et ce, dans le but de rendre automatique l'analyse des images captées par les caméras, jusqu'à présent réalisée par des humains.

Il est important de noter que les images de vidéosurveillance privée peuvent aussi être utilisées dans des procédures judiciaires. Banques, commerces, particuliers, etc : on observe une multiplication de ce genres de caméras de vidéosurveillance. Elles doivent normalement faire l'objet d'une autorisation du préfet préalable à leur installation, en justifiant par exemple la nécessité de surveiller les abords des locaux. Les caméras de particuliers ne sont pas autorisées à filmer la voie publique mais en pratique c'est de plus en plus le cas. On imagine que l'utilisation de ces images par les flics peut être contestée face à un tribunal.

En tout cas les images privées peuvent être réquisitionnées par les flics au cours d'une enquête de voisinage, ou communiquées spontanément par des propriétaires zélés. Il faut aussi penser à se méfier des interphones équipés de caméras dont certains filment en permanence ou se déclenchent avec le mouvement, disposent d'une vision nocturne, et peuvent enregistrer les images. Aux États-Unis la filiale Ring d'Amazon a des partenariats avec les flics : ces derniers peuvent solliciter n'importe quel utilisateur de leurs sonnettes connectées se trouvant dans un rayon de 400 mètres d'un délit. Ils peuvent ainsi collecter jusqu'à 12h d'enregistrement, sans mandat. En France on n'en est pas là mais on a pu par exemple voir des images d'interphone fournies à posteriori aux flics dans l'affaire d'Ivan en région parisienne en 2022[1]. Le temps de conservation des images de toutes les caméras privées est en théorie soumis au maximum de 30 jours comme les caméras publiques.



1 *Le vélo et le feu. Sur des incendies de véhicules de grandes entreprises et du corps diplomatique — et sur l'arrestation d'un compagnon anarchiste.* Brochure trouvable sur le site infokiosque : https://infokiosques.net/spip.php?article1973

5.3 QUE FONT LES OPÉRATEUR-RICE-S ?

• Contrôle à distance des caméras

Concrètement, un-e opérateur-rice a devant les yeux : un plan avec toutes les caméras, un écran de visualisation, ainsi qu'un joystick (cf. image p. 42). Ses opérations sont ainsi très basiquement les suivantes. Iel sélectionne une caméra sur une carte. Iel la visualise sur l'écran de visualisation. Iel peut ensuite zoomer ou diriger la caméra si celle-ci possède un zoom et est mobile à l'aide du joystick afin de surveiller plus précisément un espace. Si l'opérateur-rice a repéré un « délit » ou une « incivilité » sur le plan d'une caméra mais que sa cible sort du champ de celle-ci, iel peut tenter, à l'aide de l'interface graphique, de la traquer. Iel va alors prendre le contrôle de la caméra suivante. On notera que cette opération n'est possible qu'à condition qu'il y ait beaucoup de caméras.

• Opérations automatiques programmées

En plus de la surveillance de base décrite au-dessus des opérateur-rice-s, celleux-ci peuvent programmer les caméras de quatre manières :

Le **masquage dynamique** : il s'agit de masquer des champs de vision de la caméra – souvent les champs de vision non-autorisés d'une caméra. Cette fonction est très souvent utilisée pour masquer les espaces privés pris dans le champ de caméras publiques. Ce qui est légalement toujours censé être le cas.

La **préposition** : cette fonction consiste à fixer des positions d'une caméra mobile. Il est également possible de fixer plusieurs positions selon un certain cycle avec des temporisations. La caméra passe ainsi tant de temps sur un champ, tant de temps sur un autre et ce, de façon programmée.

La **mémorisation d'un cadrage** : lorsqu'un-e opérateur-rice pilote une caméra, iel peut mémoriser un point d'intérêt (cadrage) de manière à pouvoir y revenir, par une manœuvre simple, à sa convenance après avoir manipulé cette même caméra ou après son redémarrage en cycle.

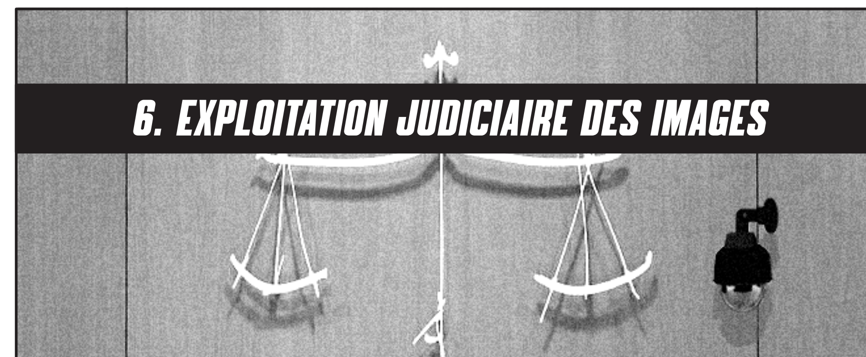
La **caméra figée** : cette fonction permet de figer, par une manœuvre volontaire, une caméra sur une scène particulière. La caméra ne sera libérée que par une nouvelle action volontaire de l'opérateur-rice.

• Signalements aux keufs

Une des opérations majeures des opérateur-rice-s consiste à faire des signalements aux flics (à l'exception de la vidéo-verbalisation où celleux-ci sont habilité-e-s à verbaliser seul-e-s, il leur suffit de relever les plaques des véhicules).

Une fois l'illégalisme ou l'individu « anormal » repéré, le rôle de l'opérateur-rice va alors être de le signaler, éventuellement de suivre l'intervention des forces de l'ordre en direct, voire même de les guider dans leur intervention. Dans ce dernier cas, l'opérateur-rice non seulement signale un évènement, mais réalise un suivi de l'individu afin de guider les keufs.

Dans certains CSU, comme celui de Vitrolles (13), il a été mis en place un système permettant de renvoyer en direct les images aux keufs. Ce qui rend possible le suivi par la police elle-même et non plus par le CSU. Dans ces commissariats, il est possible pour les keufs non seulement d'avoir les images en direct, mais également de « prendre la main sur une caméra et de la piloter de manière autonome si nécessaire ». Dans certaines villes comme Crépy-en-Valois (60) ou à Bagnolet (93), les flics municipaux ont même accès aux caméras de vidéosurveillance partout dans la ville sur leurs tablettes numériques grâce à un réseau wi-fi « hypersécurisé » qui leur donne accès aux images sur demande. On voit donc que les modalités de signalements et de renvois des images en direct sont diverses : parfois ce sont les opérateur-rice-s qui signalent et opèrent le suivi, parfois sont mis en place des systèmes de transmission des images voire de pilotage des caméras par la police nationale elle-même.



On a vu le cas de la visualisation des images en direct. En ce qui concerne la visualisation des images a posteriori dans le cadre d'exploitations judiciaires, plusieurs choses sont à savoir. D'abord, les images ne sont conservées que trente jours au maximum, délai au-delà duquel elles doivent être supprimées sauf si elles ont été réquisitionnées par la justice. Chaque CSU définit son propre délai de conservation des images (souvent entre une quinzaine et trente jours). Ensuite, les images ne peuvent être transmises aux services de police que dans le cadre d'enquêtes de police judiciaire : procédure de flagrance, enquête préliminaire et information judiciaire. À cela il existe une exception prévue par la loi qui concerne les « cas d'urgence et d'exposition particulière à un risque d'actes de terrorisme ». Cependant dans les faits les services de vidéosurveillance fournissent parfois des images en dehors de tout cadre légal. On pense par exemple à Benalla en 2017 qui a eu accès à des images de vidéosurveillance sans réquisition judiciaire.

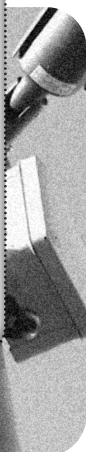
La remise des images aux keufs répond à certains critères : elle doit être faite en mains propres et matériellement ; il ne peut y avoir de coupure dans les séquences ; les images ne peuvent être dégradées ; elles sont souvent faites sur un support non réinscriptible (généralement une clé USB ou un CD) ; les images sont dans des formats qui ne peuvent être lus sur des lecteurs standards du marché. Les flics font ensuite une description des images sous forme d'un procès-verbal éventuellement agrémenté de captures d'écran, qui est versé au dossier (ainsi que le support sous scellé).

public. Et de nouvelles communes non encore équipées sont sur le point de le faire et de s'intégrer au système. Dès 2014 des capteurs ont été installés à Strasbourg à titre expérimental. Mais comme souvent, ils sont restés en place. Ils permettent de détecter une signature sonore correspondant à une « situation pouvant porter atteinte à la tranquillité publique, dans le cadre de la vie nocturne », ce qui alerte les agents visionnant les caméras.

Le Centre intercommunal urbain de vidéoprotection à Nîmes est un réseau mutualisé de près de 1 000 caméras, avec vingt agents qui veillent 24h/24 et 7j/7 sur les vingt-deux communes de Nîmes métropole. Devant une mosaïque de trente-trois écrans, pouvant afficher chacun jusqu'à 24 images, cinq équipes de quatre opérateur-rice-s se relaient.

Les halls d'immeuble

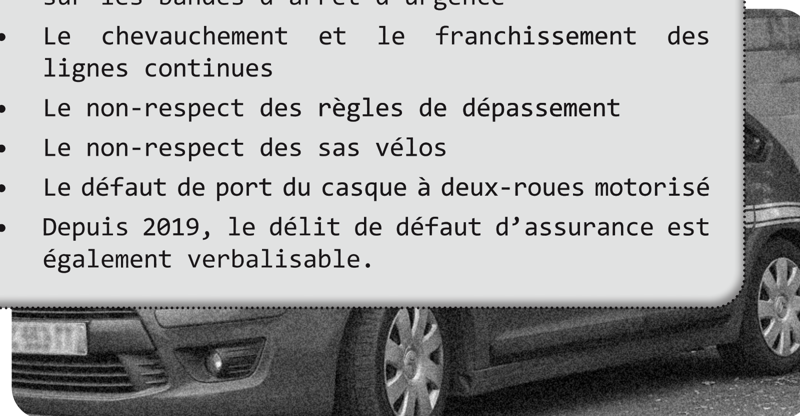
Le visionnage en temps réel des caméras de halls d'immeubles habitatifs peut être transmis aux flics sur décision des copropriétaires en cas d'occupation des parties communes. En cas d'« urgence » suite à une alerte du gestionnaire de l'immeuble, les flics peuvent se passer de l'autorisation des propriétaires.



La vidéo-verbalisation

La vidéo-verbalisation permet à des opérateur-rice-s assermenté-e-s de constater sur leur écran de contrôle des infractions au code de la route filmées par une caméra. Des images du véhicule, de sa plaque et potentiellement de ses occupant-e-s sont capturées pour prouver l'infraction. L'opérateur-rice édite alors, par voie électronique, le procès verbal, qui donnera lieu à une contravention au domicile de la personne titulaire de la carte grise. Les infractions qui peuvent être constatées sont les suivantes :

- Le non-respect des signalisations imposant l'arrêt des véhicules (feu rouge, stop…)
- Le non-respect des vitesses maximales autorisées
- Le non-respect des distances de sécurité entre les véhicules
- L'usage de voies et chaussées réservées à certaines catégories de véhicules comme les bus et les taxis
- Le défaut du port de la ceinture de sécurité
- L'usage du téléphone portable tenu en main
- La circulation, l'arrêt, et le stationnement sur les bandes d'arrêt d'urgence
- Le chevauchement et le franchissement des lignes continues
- Le non-respect des règles de dépassement
- Le non-respect des sas vélos
- Le défaut de port du casque à deux-roues motorisé
- Depuis 2019, le délit de défaut d'assurance est également verbalisable.



5.4 LA MUTUALISATION DES SYSTÈMES DE VIDÉOSURVEILLANCE

Depuis quelques années, de nombreux politiciens, gestionnaires et autres VRP de technologies de contrôle encouragent à développer des modes de mutualisation de la vidéosurveillance avec le double objectif de réduire ses coûts, et de l'étendre à une zone géographique plus large. Parfois ces souhaits se sont heurtés à une législation un peu restrictive à leur goût. Mais depuis la loi de 2007 relative à la prévention de la délinquance, puis avec la loi sécurité globale de 2021, les dernières barrières semblent être tombées. Aujourd'hui, les différentes collectivités territoriales, que ce soient les EPCI (établissements publics de coopération intercommunale), ou les syndicats mixtes qui sont différentes formes de coopération entre communes, peuvent acquérir, installer et entretenir un dispositif de vidéosurveillance mutualisé. Il s'agit de transmettre à un CSU intercommunal des images captées sur la voie publique ou dans les lieux ouverts au public sur le territoire des communes membres. Ces images sont ensuite exploitées, au travers d'un visionnage et d'un enregistrement centralisés, par des agents de police municipale, mais aussi désormais par des agents territoriaux.

Les conseils départementaux et les conseils régionaux peuvent également mettre en œuvre un système de vidéosurveillance autour des bâtiments et installations publics relevant de leur domaine et dont elles assurent la gestion (collèges, lycées, routes, bâtiments administratifs).

Pour autant, ces mutualisations ne semblent pas encore être la règle. Mais l'AN2V (Association nationale de la vidéoprotection), mène d'ores et déjà campagne pour encourager le déploiement de la vidéosurveillance en convainquant les élus locaux d'adhérer à ces projets de mutualisation. Il s'agit pour eux d'éviter « les trous dans la raquette dans le continuum de sécurité », notamment en ayant la possibilité de suivre des déplacements d'une commune à l'autre. Mais également de lutter contre le phénomène des « caméras passives » dont les images ne sont pas visualisées et ne sont exploitables que sur réquisition des services de police et de gendarmerie, alors qu'avec un CSU et ses agents derrière les écrans, les forces de l'ordre et le

maire peuvent être alertés en temps réel. Une des cibles de l'AN2V sont les quelques 35 000 communes de moins de 10 000 habitants en France, des communes rurales et périurbaines qui n'ont pas les moyens de se doter d'un CSU. Pour les convaincre, l'AN2V mise sur une vidéosurveillance automatisée toujours plus sophistiquée. Elle permet de diminuer le nombre d'opérateur-rice-s qui ne seront plus obligé-e-s de scruter un nombre important d'écrans, mais recevront des alertes signalées par l'ordinateur.

En attendant, il existe déjà quelques exemples qui nous donnent une idée de ce que cette mutualisation rend possible (la mutualisation pour Paris et les villes aux alentours sera détaillée dans la partie 8).

La communauté d'agglomération Plaine vallée (18 communes et 183 806 habitant-e-s), dans le Val-d'Oise, fait partie des collectivités pionnières. Depuis 2007, elle a mis en place un dispositif intercommunal de vidéoprotection, doté de 212 caméras pour l'ensemble du territoire (75 km²), complétées par 18 caméras nomades. 23 opérateur-rice-s se relaient 24h/24 et 7j/7 dans deux CSU.

Seine-et-Yvelines Numérique (SYN) est un syndicat mixte ouvert qui réunit des adhérent-e-s tels que deux départements d'Île-de-France (Hauts-de-Seine et Yvelines), une trentaine de communes de ces deux territoires, 9 intercommunalités, et des membres tels que le SDIS 78 (Service départemental d'incendie et de secours des Yvelines). La mutualisation des services de vidéoprotection des établissements publics fait partie de ses missions. Celle-ci a commencé par les caméras des quelques 116 collèges du département des Yvelines, 70 bâtiments administratifs et 43 casernes de pompiers. Plus de 1900 caméras ont déjà été installées. Grâce à la loi sécurité globale, SYN compte maintenant développer la vidéoprotection mutualisée de l'espace public, c'est à dire relier les systèmes de chaque ville. D'abord en phase pilote sur quelques villes et intercommunalités en 2022, puis généralisé, à la demande, en 2023.

Le Centre de supervision de l'Eurométropole de Strasbourg assure la gestion de 426 caméras de voie publique début 2022, sur 25 communes, ainsi que plus de 300 dans des lieux accueillants du